Next Generation Networks

A. H. S. Adel
S. Å. Arntzen
K. Fagerbekk
L. N. Gustavsson
M. Lindvall
K. Nordnes
M. Skjetne
M. Skyttemyr
M. Steiro

Dec 17, 2021

Abstract

New technologies are set to change the technological landscape as we know it today. The introduction of the fifth-generation technology standard for cellular networks (5G) and Internet Protocol version 6 (IPv6) will change how we use the internet and introduce new possibilities previously thought impossible. Along with these technologies others are developed to accommodate them such as Software-defined networking (SDN) and IEEE 802.11ax commonly known as Wi-Fi generation 6. On the other side of the spectrum, we examine the low-power wide-area network modulation technique (LoRa) and its relation to 5G. Is it a competitor to Narrowband IoT, or can it be integrated as part of 5G? This paper aims to give a high-level understanding about how these technologies work, what they will be able to offer us, and finally, we examine them from a security standpoint in order to give the reader an insight about what risks to expect when implementing and using these technologies.

CONTENTS

CHAPTER ONE

INTRODUCTION

With the advent of the new telecommunication standard 5G and the most recent version of the internet protocol IPv6, we are on the cusp of a technological revolution that will change the cyberspace for years to come. These disruptive technologies will not only try to improve on the existing services that 4G and IPv4 provide, but they will also lead to new possibilities previously thought impossible.

As part of the three primary use cases of 5G NR – proposed by 3GPP – the first commercial 5G service to launch will be the eMBB (Enhanced Mobile Broadband). eMBB acts as the natural evolution of the previous 4th generation broadband cellular network technology, providing higher bandwidth and capacity. eMBB will for the most part benefit the user by enhancing the user experience. Not only will 5G ultimately improve the user experience for the general public, but it will positively influence several massive industries as well, hence the "revolution".

This revolution will partly take form in the other two use cases of 5G NR, namely mMTC and URLLC. mMTC stands for massive Machine-Type Communication which as the name suggests will allow a massive number of interconnected devices to communicate with each other. mMTC will facilitate the development of smart cities among other things. URLLC stands for Ultra-Reliable Low-Latency Communication and is a service which aims to have low latency, high throughput, and high availability. As we will see in Chapter 4 URLLC is being developed for mission-critical uses cases like industrial automation, driverless cars, and real-time control over devices like drones.

While it is true that we have 5G enabled phones and service providers marketing 5G today, we are still several years away from implementing all the features of 5G. Most service providers today have only deployed Non-Standalone 5G stations, which practically only increase data transfer speed and covers the use case eMBB. Standalone (SA) 5G has been deployed in countries like China and South Korea, but the majority of other carriers in other countries are still testing and developing SA [1]. This gives us an opportunity to develop security requirements as part of the design of SA 5G rather than an afterthought. Chapter 7 will cover the risks associated with the emergence of these technologies. While Chapter 8 will discuss solutions to the security challenges of 5G. Chapter 5 will cover LoRa and its relation to 5G as well as the security of the technology.

On the other side of the spectrum, we have the IPv6 which also will play a large part in the next generation network. Since 2011 the IPv4 addresses have been exhausted, and the switch over to IPv6 is, as we will see in Chapter 3, is still in the early stages. As with any transitions, or changes for that matter, they introduce both possibilities and challenges. It is therefore necessary to understand not only the general implementation challenges we are facing with the adoption of IPv6 globally, but also the implications they have from a security standpoint.

Chapter 6 aims to give an overview of these security challenges, as well as a short overview of the implementation of the protocol, and some proposed solutions to these challenges. Another technology that may have an interesting application as a consequence of increased 5G adoption is SDN, which will be the topic of Chapter 9.

CHAPTER

TWO

IPV6 TODAY

2.1 Introduction

In the early days of the Internet, Internet Protocol version 4 (IPv4) was used to address nodes on the various networks of which the Internet consisted. While IPv4 offers 32-bit addresses, with a capacity for just over 4 billion hosts spread over 16.7 million networks, the rapid growth of the Internet exceeded what even the most farseeing developers of the original IPv4 and TCP/IP specifications had anticipated. In 1987, estimates were made that the Internet would have a need to address up to 100,000 separate networks at some point in the future, a mark that was reached already in 1996. Exacerbating the problem was the fact that IPv4 addressing inherently had inefficiencies, originating from the large block sizes of Class A, B, and C networks that was in use at the time as a result of classful addressing. In August 1990, Frank Solensky, Sue Hares, and Phill Gross predicted that Class B address space would be exhausted by March 1994, and assigning multiple Class C networks in place of Class B networks to try to alleviate the problem, by itself caused problems, due to rapid increases in the size of the Internet backbone routers' routing tables. [2]

During the 1990s, engineers at the Internet Engineering Task Force (IETF) started to work on selecting a successor to IPv4 in an effort to overcome these challenges. This new successor would be called the "IP Next Generation" (IPng), and a task force was made to make a decision between the various candidates for IPng. In order determine the scope of IPng, a reasonable estimate was needed of the time remaining until the IPv4 address space was exhausted. The IETF formed the Address Lifetime Expectations Working Group (ALE) in 1993 to develop this estimate, and by March 1994, they had determined that the entire IPv4 address space of the Internet would be exhausted between 2005 and 2011. At the same time, considerations had to be made on how to handle the rapid growth of the existing IPv4 routing tables, which before the implementation of Classless Inter-Domain Routing (CIDR) was growing significantly faster than development of memory technology. [2]

In order to determine which technical requirements should apply to IPng, the IETF issued a call for white papers for IPng, soliciting opinions "about the various factors involved in the IPng definition and selection process" and any "issue or issues that the author feels should be understood during the IPng process." [3] The call solicited considerations regarding engineering issues such as scaling, transition, security, routing, applicability, and robustness. In response, the IETF received 21 white papers from various industries, including "the cable TV industry, the cellular industry, and the electric power industry" in addition to papers dealing with "military applications, ATM, mobility, accounting, routing, large corporate networking, transition implementations, as well as a number of other issues."

[2] These white papers, along with a Birds of a Feather meeting (BOF) in 1994, various discussions in the IPng Area, and several discussions on mailing lists together resulted in a draft IPng technical criteria document consisting of 19 core criteria for IPng proposals. [2]

By this point, multiple proposals for IPng were in the works at IETF, several of which merged over time to form three proposals: Common Architecture for the Internet (CATNIP), Simple Internet Protocol Plus (SIPP), and TCP/UDP Over CLNP-Addressed Networks (TUBA). These proposals were evaluated by the IPng Directorate on May 19th and 20th 1994 in Chicago. CATNIP was largely considered to be incompletely specified, though was noted as having many innovative ideas. SIPP was considered by most of the reviewers, as one reviewer put it, an "aesthetically beautiful protocol well tailored to compactly satisfy today's known network requirements," but notably had a flawed transition plan, one that was "fatally flawed and could not be made to work reliably in an operational Internet." [2] TUBA had the advantage that, being CLNP-based, many CLNP-capable routers were already deployed on the Internet, as well as the protocol's "potential for convergence of ISO and IETF networking standards," [2] however, a major point of contention was whether IETF could make modifications to the protocol, or whether any changes had to go through the ISO standards process.

In the time that followed the Chicago retreat, considerable discussion took place around the strength and weaknesses of the protocols. The SIPP working group published a revised version of SIPP that was submitted to the IPng Directorate for evaluation, representing "a synthesis of multiple IETF efforts with much of the basic protocol coming from the SIPP effort, the autoconfiguration and transition portions influenced by TUBA, the addressing structure is based on the CIDR work and the routing header evolving out of the SDRP deliberations." [2] After considerable discussion, the SIPP protocol as described in "Simple Internet Protocol Plus (SIPP) Spec. (128 bit ver)," was recommended with the consensus of the IPng Directorate to be adopted as the basis for IPng, the next generation Internet Protocol. This generation of the Internet Protocol was assigned as Internet Protocol version 6 (IPv6) by IANA, and designated as the successor to IPv4. [2]

2.2 IPv6 as a protocol

Compared to IPv4, IPv6 primarily differs in five aspects. Firstly, and the most notable, is IPv6's expanded addressing capabilities. Whereas IPv4 had an address size of 32 bits, IPv6 uses a 128 bit address size "to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler autoconfiguration of addresses." [4] IPv6 also offers improved multicast routing scalability over IPv4 through its "scope" field, and further adds an entirely new type of address known as "anycast" addresses, wherein a packet is sent to "any one of a group of nodes." [4] Unlike IPv4, IPv6 does not have broadcast addresses, due to their function being superseded by multicast addresses. [5]

The choice of address size was one of the most hostly discussed aspects when designing IPng, with four distinct views being expressed. The first view was that "8 bytes of address are enough to meet the current and future needs of the Internet," and that "more would waste bandwidth, promote inefficient assignment, and cause problems in some networks." The other was that 16 bytes is "about right" and that such a length "supports easy auto-configuration as well as organizations with complex internal routing topologies in conjunction with the global routing topology now and well into the future." Some had the view that "20 bytes OSI NSAPs should be used in the interests of global harmonization," while a fourth view was that “variable length addresses which might be smaller or larger than 16 bytes should be used” as a way to harmonize and embrace the other three views. 16 bytes of address was chosen, not unanimously, but because 16 bytes was the view held by the majority, offering the best compromise between the options. [2]

Another aspect in which IPv6 differs from IPv4 is in its simplification of the header format. Several headers fields that were present in IPv4 have been dropped or made optional in IPv6, in an attempt to reduce the processing required for packet handling, and limiting the bandwidth cost of the IPv6 header. The only required headers in IPv6 are the IP version, traffic class, flow label, payload length, next header field, hop limit, and source and destination addresses. [4] IPv4 fields such as the time-to-live, header checksum, options, and fragment offset [6] are not required in IPv6. Instead, IPv6 can specify through its “next header” field if any optional headers are included in the packet. If the “next header” field of the first header in the IPv6 packet is set to e.g. TCP, then TCP data will directly follow that header. However, the “next header” field can also be set to indicate for example the “fragment” next header, or “routing” next header, to indicate that such headers follow the initial IPv6 header. Those following headers can then specify an additional “next header” field, leading to a chain of headers and references to the next header, until the upper protocol layer is encountered by e.g. a reference to TCP as the next header. [4]

These headers are called “extension headers,” and their encoding represents the third major change from IPv4. Extension headers are “not processed, inserted, or deleted by any node along a packet’s delivery path, until the packet reaches the node (or each of the set of nodes, in the case of multicast) identified in the Destination Address field of the IPv6 header.” [4] The only exception to this is the “hop-by-hop options” header, which “is not inserted or deleted, but may be examined or processed by any node along a packet’s delivery path,” and specifies options to be processed or examined by each node the packet passes through. [2, 4] The IPv6 changes to extension headers and options allow for “more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.” [4]

The fourth major change in IPv6 is the introduction of flow labeling. This capability is added “to enable the labeling of sequences of packets that the sender requests to be treated in the network as a single flow.” [4] A flow in this regard is considered from a network layer viewpoint as “a sequence of packets sent from a particular source to a particular unicast, anycast, or multicast destination that a node desires to label as a flow,” and from an upper-layer viewpoint as something that consists of “all packets in one direction of a specific transport connection or media stream.” [7]

Traditionally, classification of flows has been done using the source and destination addresses and ports, together with the transport layer protocol type. This is problematic notably due to the fact that these fields may not always be available due to fragmentation or encryption, and limits classifications to transport layer protocols that the node is aware of. [7] Furthermore, it would make it impossible to distinguish between multiple flows within tunneled traffic, as the outer encapsulation of the traffic will always have the same addresses and ports. An example of when this is problematic is when link aggregation (LAG) or equal cost multipath routing (ECMP) is used to aggregate capacity, wherein certain goals must be met – maintenance of “roughly equal share of traffic on each path,” minimizing out-of-order delivery for individual flows, and minimizing idle time on “any path when the queue is non-empty.” [8] Using IPv6, the tunnel endpoint can determine the different flows of traffic within the tunnel and assign a flow label to each encapsulated stream, maintaining any confidentiality or encryption of the tunneled traffic, but still allowing link aggregators to distinguish between flows inside the tunnel. This enables the aggregator to split the encapsulated tunnel between multiple different links or routing paths, without causing flows inside the tunnel to be fragmented between routes.

The IPv6 extensions for authentication, data integrity, confidentiality, and privacy constitute the fifth major change over IPv4, now being specified for IPv6. Through use of the IP Authentication Header (AH) [9], IP Encapsulating Security Payload (ESP) [10], and IPsec [11]; confidentiality, integrity, and authentication is ensured for traffic that implements these extensions in IPv6. IPv6 defines the order of these headers relative to the other extensions in the IPv6 specification. [4]

2.2.1 Address autoconfiguration

Many IPv4 networks have traditionally employed the dynamic host configuration protocol (DHCP) to allocate IP addresses to devices. DHCP is builds on the server-client model, with a DHCP server that "[allocates] network addresses and [delivers] configuration parameters to dynamically configured hosts" [12], or clients. DHCP for IPv4 supports three modes of allocating addresses – automatic allocation, wherein a permanent IP address is assigned to a client; dynamic allocation, where an IP address is assigned to a client for a limited amount of time; and manual allocation, where the network administrator assigns IP addresses, and DHCP merely conveys these to the clients. [12] DHCP also exists for IPv6 (known as DHCPv6) [13], but has more limited use for address allocation compared to IPv4 due to IPv6's usage of SLAAC. As such, the SLAAC mechanisms are worth exploring to gain an overview of how addresses are allocated in IPv6.

SLAAC, or stateless address autoconfiguration, is a set of steps performed by hosts in IPv6 to automatically assign IP addresses to their interfaces. The mechanism is designed to require "no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers." [14] The information required by hosts to generate addresses is sourced using a combination of locally available, and router-advertised information. In IPv6, all interfaces have a link-local address [15] which by itself is sufficient for communicating with other nodes on the same link. This address is generated using SLAAC, is stateless, and is configured based on an "interface identifier" generated by each host whenever the interface is enabled. This occurs in four scenarios: when then interface "is initialized at system startup time;" whenever it is "reinitialized after a temporary interface failure or after being temporarily disabled by system management;" upon being attached to a link for the first time, including the case where "the attached link is dynamically changed due to a change of the access point of wireless networks;" and whenever the interface "becomes enabled by system management after having been administratively disabled." Such addresses are always allocated from the fe80::/16 prefix, and have infinite preference and validity lifetimes. [14]

Global addresses can also be allocated using SLAAC. In this case, the router will periodically send router advertisements (RAs) to the all-nodes multicast address (ff02::1), as well as in response to any router solicitation packets sent to the all-routers multicast address (ff02::2). RAs are ICMPv6 packets that contain the router's link-local address and a destination address (or all-nodes multicast address) for the packet, as well as prefix information that client nodes can use to generate a global address for its interfaces. [14, 16]

In all cases where SLAAC is being used, be it for link-local or global addresses, the host must perform duplicate address detection to avoid assigning an address to any of its interfaces that is already in use by another host on the link. This is because the host chooses its own addresses for its interfaces with no specific authorization for picking any particular address by a governing server, due to SLAAC's stateless nature. Duplicate address detection is performed by sending neighbor solicitation and advertisement messages on the link for which the address should be allocated. This process is fairly simple in nature – the host sends a neighbor solicitation packet to the address it wishes to use, and if a response is received, the address is already in use by another interface on the link. In this case, the host has to choose another address for the interface and perform duplicate address detection on the new address, until an address is picked that is not in use.

While SLAAC always takes place for link-local addresses, network administrators may opt to deploy DHCPv6 instead of, or in combination with, SLAAC for global addresses. Whether or not SLAAC is used for address allocation in DHCPv6 determines whether or not the network uses stateless or stateful address allocations. As DHCP has many more uses beyond address allocation, such as advertising DNS servers, it is possible for a network to rely on SLAAC for address allocation, while still using DHCP for configuring other properties of a networked host. This is called stateless DHCP, and is considered "the simplest and most basic operation for DHCP" in IPv6 [13]. Stateless addressing is useful for networks where the site is "not particularly concerned with the exact addresses hosts use, so long as they are unique and properly routable." [14]

The opposite approach to using SLAAC with DHCPv6 is to have the DHCP server allocate addresses for clients on the link from a prefix address pool. This is called stateful DHCP, and matches the mode of operation that originally motivated the creation of DHCP for IPv4. Stateful DHCPv6 is appropriate for situations where "stateless address autoconfiguration alone is insufficient or impractical, e.g. because of network policy, additional requirements such as dynamic updates to the DNS, or client-specific requirements." [13]

2.3 IPv6 adoption

As previously explained in the introduction to this paper, IPv6 was designed and developed due to IPv4's inherent scaling problems, such as the depletion of address space for devices connected to the Internet. However, the current consensus appears to be that IPv6 adoption is rather slow. There are few business drivers that actively encourage ISPs and service providers to transition to IPv6, and penetration of IPv6 for end users has been very limited except for certain areas in Europe, and other technologies such as carrier-grade NAT has been increasingly employed as a way to stagnate IPv4 address depletion in consumer-focused IP networks. Despite this, there are several market drivers that are causing change in the IPv6 for consumers landscape, of which five can be considered core drivers, that will be explained more in depth in the following paragraphs. [17]

The first of the five primary drivers is the depletion of IPv4 address space. When IPv4 addressing was first conceived, nobody could envision that we would end up in a society where cars, phones, toasters, refrigerators, TVs, and even lawn mowers would be connected to the Internet. IP addresses are delegated by regional internet registries (RIRs), and as of 2020, ARIN, LACNIC, and RIPE NCC, or the North and South American and European RIRs respectively, have depleted their unallocated addresses pool. This means the Asia-Pacific and African RIRs, APNIC and AFRINIC, are the only RIRs with any amount of unallocated IPv4 addresses left, allocating from their last /10 and /11 address blocks respectively. As a result of this, already allocated blocks of IPv4 address space are now being sold and leased between providers instead of being assigned by RIRs directly. [18] This in turn means

RIRs can only hand out new IPv6 assignments, which is expected to boost IPv6 adoption in markets that are affected by the exhaustion. [17]

The second primary driver is the support of IPv6 in major operating systems. All major operating systems currently support IPv6, with support enabled by default. In desktop computing systems, this support has been in place on Windows since 2007, on Linux since 2005, and on OS X since 2002. [17] Since support has been in place for such a long time, devices will be able to take advantage of IPv6 immediately.

Another considerable market driver is the rise of cloud-based computing. IPv6 is particularly important for cloud solutions, because of its potential for scalability and how it can solve key constraints for service providers. The cloud providers Amazon and Azure both support IPv6 in their cloud service offerings, and all major networking hardware, OS and hypervisor and cloud management vendors support IPv6. By using IPv6, network address translation managements and IP range conflicts both become a thing of the past, with a practically unlimited amount of globally unique addresses available for cloud service infrastructure. IP address conflicts, overlapping address space and subnet size limitations are not problems that need to be considered in IPv6. [17]

Similarly to cloud providers, mobile computing is expected to be a major market driver for IPv6. The rapid increase in communication capacity, number of connected devices, and growth of the Internet of Things in data-based mobile networks means IP address requirements for mobile network operators has exploded. Several mobile networks are mandating IPv6 support, as it is the only way to effectively address the rapid adoption of mobile, smart, and embedded devices entering the market. [17]

Lastly, access to reference materials on the implementation of IPv6 is finally being significantly improved. Until a few years ago, the lack of reference materials for deployment of IPv6 in enterprise networks meant that few network administrators were willing to or able to implement IPv6 in their networks. Now that materials are available, IPv6 support in hardware and software has matured, and guidance from both vendors and third parties ensures configuration of IPv6 is now much easier for network administrators moving forward. [17]

One business driver that has been pointed out as a major driving force behind adoption of IPv6 by enterprise organizations is business continuity, specifically for those that deal with businesses in the Asia-Pacific region. Because many parts of APNIC's coverage area is now only getting IPv6 address allocations, IPv6 is crucial for doing business with many businesses in this area. Many enterprises use "an application delivery controller (ADC) or a content delivery network (CDN) to translate from an IPv6 request to an IPv4 resource." [17] It would be much more efficient if more services were available natively on IPv6.

2.3.1 Slowing IPv4 address exhaustion

While IPv6 was being developed to counter address depletion, other measures had to be taken to slow address exhaustion in the IPv4 address space. One of the first such measures was the introduction of network address translation (NAT) in 1994. NAT was developed in addition to classless inter-domain routing (CIDR) as a short-term solution to the address the exhaustion problem, but like the other short-term solutions, it would only delay the eventual depletion of address space until IPng, the long-term solution, was finalized. NAT was designed as means of reusing addresses in cases where only a small percentage of hosts communicate outside of their networks, and thus only a few globally unique IP addresses would be needed to the network. [19]

NAT works by assigning a pool of globally unique IP addresses to the edge router of a network, known in NAT terminology as a stub router. All hosts in the network behind this stub router, known as the stub network, instead get private, non-globally-unique IP addresses that are only valid within the scope of that stub network. [20] The addresses typically used for these purposes are the three prefixes 10/8, 172.16/12, and 192.168/16, allocated by the Internet Assigned Numbers Authority for private internets. [21] When a host in the stub network desires to connect to an external network, it sends a normal IP request to the given destination address to the stub router that acts as the gateway for the network. When the stub router receives this request, it replaces the source address of the packet with one of the addresses in its global address pool, and internally maps the IP address of the requesting node to the globally unique address that is temporarily assigned to the originating host. The destination host will see traffic originating from the stub router, and when a response is received, the stub router translates the globally unique address back to the private internet address that is permanently assigned to the originally requesting host. This way, a device can be virtually assigned a globally unique address on the router, and traffic can flow from this device to other networks normally despite the originating host having a private internet address. [20]

As noted in the original specification for NAT, this approach has some disadvantages. Notably, it is "taking away the end-to-end significance of an IP address, and making up for it with increased state in the network." [19] However, one of the more pressing concerns is that the number of hosts in the stub network that can access other networks simultaneously is limited to the total number of globally unique addresses that the stub router has allocated to it in its pool for NAT usage. In today's world, most networks are only allocated a single globally unique IP address, and with a large number of connected clients, a single host in the stub network being able to communicate out to other networks at a time is simply not feasible. A solution to this was created called network address port translation (NAPT), also known as port address translation (PAT).

NAPT works by mapping tuples of TCP/UDP port numbers and stub network IP addresses to other TCP/UDP port numbers on one or more globally unique IP addresses. In this way, NAT mappings are created on a port-by-port basis rather than on a host-by-host basis. An unfortunate side effect of NAPT is that only TCP/UDP sessions are allowed, and they must originate from the stub network. Using port forwarding, traffic destined to well known ports on the globally unique IP address(es) assigned to the stub router could be configured on the router to be forwarded to a specific node on the stub network. Some protocols' traffic, such as FTP, also have to be modified by the stub router in transit to work properly, because they embed IP addresses and/or port numbers in their protocol data that represent a private internet address rather than a globally unique one. NAT also has various security problems that this paper will not go into further detail on, as they are not in scope for explaining IPv6. [20, 22]

2.3.2 Carrier-grade NAT

Despite NAPT allowing multiple devices to simultaneously connect to external networks through a single, shared IP address, it has not on its own been an effective countermeasure at the consumer level. More and more households are being connected to the Internet, and host-based transition mechanics were by themselves not able to meet the requirements in all cases. In an effort to further delay IPv4 address exhaustion, carrier-grade NAT (CGN) was designed wherein NAT is applied at the ISP level, and customers are allocated private IP addresses from their service providers. With a second NAT located at the customer's edge router, CGN results in two layers of NAT being applied to traffic. [23]

While CGN is a useful stop-gap for internet service providers to share its IPv4 address space across more consumers, it "compounds IPv4 operational problems when used alone but does nothing to encourage IPv4 to IPv6 transition." Furthermore, "deployment of NAT444 CGN allows ISPs to delay the transition and therefore causes double transition costs (once to add CGN and again to support IPv6)." [24] Beyond increasing costs and delaying IPv6 adoption, this type of address sharing also gives rise to a significant number of other issues inherent in the operation of network address translators on the Internet, including issues for "end-users, service providers, and third parties such as law enforcement agencies and content providers." [25] This paper will not comprehensively cover all of these issues, but will seek to explain a handful of them in some detail.

The first issue that comes to light when a large number of subscribes share a single, or small number, of globally unique IP addresses is that NAPT breaks down when there are too many outbound connections from the internal pool of users that the NAPT's allocation pool can cover. The outgoing port for TCP and UDP traffic is usually not relevant, and NAPT will allocate ports on its globally unique address(es) for outgoing traffic that does not guarantee correspondence with the original source port of the traffic. However, the amount of connections that a NAPT can sustain, and by extension the amount of simultaneous connections from customers behind a CGN, is limited by the number of ports available across the pool of globally unique addresses assigned to a CGN. [25] Ports in TCP should not be re-used even several minutes after the connection is closed, due to risks of overlap of TCP sequence numbers causing overlap that can break a TCP connection in various ways. [25, 26] This also has to be taken into account when considering how much global IPv4 address space should be allocated to the CGN to sustain peak traffic from the subscriber network behind the CGN. In cases where e.g. a worm is propagating between devices on the subscriber network, a very large number of outbound connections may be established by the worm from many different devices, which can quickly exhaust the address allocations of the CGN. [25]

In order to reduce the need for a large globally unique address allocation to the CGN, IPv6 should be implemented, as deploying IPv6 to the customer networks results in traffic being offloaded from IPv4 to IPv6 in these networks. Because there is no need to perform CGN on IPv6 traffic due to the large address space of IPv6, less processing is required by the CGN, and fewer globally unique IPv4 addresses need to be assigned to the CGN to handle the outbound traffic. When a customer attempts to open a connection to a dual-stack host, and the customer device prefers IPv6 connections, the traffic that needs to be NAT-ed by the CGN is effectively reduced to only hosts that do not have IPv6 support implemented and enabled.

Inbound traffic to customer networks is much less common, but a majority of subscribers do accept at least one inbound connection. As such, a large allocation of inbound ports is not required per customer, and allocation can be done on demand using e.g. universal plug and play (UPnP) or the

NAT port mapping protocol (NAT-PMP). For this to work with CGNs, the CGN and customer edge equipment need to cooperate to open the incoming port on both the CGN and customer NAT. This can be solved using a UPnP or NAT-PMP proxy, or the Port Control Protocol (PCP). Connections to well-known port numbers will generally not work, however, when CGN is applied. For applications that can run on alternate ports, this can be worked around, but not all applications support this type of configuration. Usage of SRV records in DNS can in some cases be used to publish alternate port numbers in DNS, but such solution has historically not gained much traction. HTTP and many other protocols do not support SRV, for instance. [25]

Beyond port-related problems, applications themselves and their protocols may fail to work in the presence of a NAT or CGN. Most notably this includes applications that require inbound communications, as mentioned in the previous section, but also applications that carry address and/or port data within their protocol's payload, applications using fixed ports, applications not using any port (such as ICMP echo), applications that assume unique source addresses, and applications that prohibit multiple connections from a single address. Furthermore, all applications that use other types of IP traffic than TCP and UDP will fail to work outright, such as IPsec ESP and applications utilizing SCTP. [25]

Usage of CGN also interfere with geo-location and traceability. IP addresses are often used to provide the general location of connecting hosts, and such geo-location services "are used by content providers to allow them to conform with regional content licensing restrictions, to target advertising at specific geographic areas, or to provide customized content," and can also affect provisioning of emergency services. [25] Furthermore, CGNs can interfere with law enforcement's ability to identify a particular Internet subscriber by their IP address. When globally unique IP addresses are assigned to a particular subscriber for a long time, knowing only the originating IP address and a time stamp for a criminal event allows service providers to easily provide information about which customer that particular IP address was assigned to at the given time. However, when CGN is in place, a single address is shared by multiple subscribers and makes it ambiguous which client committed the criminal act unless the source port is also provided by law enforcement. [25]

In order for law enforcement requests to be successful, there are two different solutions that can be put in place – either, source ports must also be logged alongside the source IP address in traffic logs, or service providers implementing CGN need to continuously log destination addresses. The first solution requires accurate time-keeping because of the dynamic nature of port assignments in NAT, where even a small time skew can result in ambiguity about which customer was assigned that port at the time. It can also be unrealistic to assume that all servers will log port numbers, and as such destination IP logging on the service provider side may be preferable. However, that approach is also flawed: in cases where multiple subscribers are accessing the same service at the same time, figuring out which of the multiple subscribers is responsible for the malicious activity may be impossible, and the service provider would have to disclose the identities of a potentially significant number of subscribers to law enforcement. [25]

Usage of CGN also has direct security implications for services that use IP addresses as a basis for abuse prevention and access control. If one subscriber tries to attack a server, for example, that server could put the CGN's IP address on a blacklist, also inadvertently blacklisting all other customers of the service provider that are assigned to the same CGN IP address. Access control lists (ACLs) that rely on simple authentication via IP addresses will also fail to work, granting multiple subscribers access to a service that was only intended for one subscriber, because the subscriber shares the IP address with multiple other subscribers. [25]

2.4 Summary

The problems associated with IPv4 address exhaustion have been known since the 1990s and continue to be a growing concern today. While multiple transition methods have been proposed and implemented to alleviate address space depletion-related problems, many of these methods have proven insufficient by themselves over time. Despite increasing market drivers for IPv6, deployment has been unexpectedly slow, and many hosts are still not connected to the IPv6 Internet today. Instead, internet service providers have introduced short-term solutions like carrier-grade NAT that while somewhat effective at delaying IPv4 address exhaustion, introduce new or worsen already existing security complications of address translation, further delay implementation of native IPv6 globally, increases costs for service providers, and interferes with the ability for applications, law enforcement, emergency services, and abuse prevention to function correctly.

In the long term, implementing IPv6 globally is the only measure that will solve the IPv4 address space exhaustion issue. All modern operating systems and all major cloud providers currently support IPv6, and given that most regions in the world are now out of IPv4 addresses,

CHAPTER

THREE

GOING FORWARD WITH IPV6

Abstract

IPv6 has long been the successor to IPv4 and addresses many of the limitations of IPv4. Yet, the adoption of the new protocol has been slow. This article examines IPv6 adoption by evaluating the progress and its projection. We will describe the challenges of the adoption and look at different solutions.

This article uses sources from published reports to analyze the different aspects of IPv6. Our findings show the increasing growth of IPv6-enabled devices and providers over the past years. New technologies (like 5G and IoT) will increase the need for IPv6 and boost its adoption even further. Since IPv6 and IPv4 must coexist for some time, interoperability will be challenging. Dual-stack technology solves this problem by uniting the two protocols.

As the adoption seems to gain pace, IPv6 will dominate as the most popular network addressing protocol in the coming future.

3.1 Introduction

The Internet consists of increasingly more connected users and devices that want to communicate. *Internet Protocol version 4 (IPv4)* has for a long time been the most used protocol for addressing internet traffic. With its limited amount of address space, IPv4 has reached its limits - making addressing dependent on *Network Address Translation (NAT)*. This has long been foreseen and already in 1994 its successor, *Internet Protocol version 6 (IPv6)*, was standardized. IPv6 has a much larger address space, it's in fact 400 times larger than that of IPv4. This expansion is critical for the widespread emergence of IoT devices. The transition from IPv4 to IPv6 will be a long and tidy process were both protocols must coexist during this period. In this paper, we will look into the status of IPv6 adoption, what impact new technologies can have on the adoption, and what goals are set for the future of the protocol.

3.2 The IPv6 adoption

In this chapter, we evaluate the state of IPv6 adoption and look at existing challenges. We also look at some suggestions on how to address these challenges.

3.2.1 Evaluation

First, we look at the growth of IPv6 adoption compared to IPv4. There are different ways to measure IPv6 adoption. Some methods involve comparing prefix allocation, traffic data, and availability. We will also look at predictions for further adoption.

From the research in the article "Measuring IPv6 adoption" from 2014, they find that "Traffic data shows that IPv6, while just 0.63% of measured Internet packets, is growing at a rate of over 400% in each of the last two years" [27]. These are measurements *from March 2010 to March 2011*. It is then fair to say that especially new products are using IPv6 natively, making the adoption increase rapidly at the time of measurement. Looking at the results of this article, IPv6 still has a long way to go, but since the exhaustion of the IPv4 address space in February 2011, the adoption has become more imminent. The researchers also projected that IPv6 was becoming a significant fraction of traffic with an IPv6 to IPv4 traffic ratio between .03 and 5.0.

As expected, the IPv6 prefix allocation is outpacing the IPv4 prefix allocation as reported in 2017 [28]. From January 2014 to January 2017, IPv6 prefixes increased by 76.7% compared to a 26.2% increase for IPv4 in the same period. These are measures taken from the *Regional Internet Registries (RIRs)*. However, prefixes must be announced in the global *Border Gateway Protocol (BGP)* routing table before being used. Numbers taken from the *University of Oregon Route Views Project* show an increase of 126.5% for IPv6 prefix announcements compared to 38% for IPv4 prefix announcements in the same period.

Google collects statistics about IPv6 adoption by measuring the availability of IPv6 connectivity among Google users. In January of 2011, 0.24% accessed Google through IPv6. Since then, the use of connections with IPv6 has reached a total of 35.83% on the 24th of October, 2021 [29].

A report from 2020 [30] looks at the current adoption of IPv6 and tries to predict the future growth of the protocol. In northern and western Europe, the IPv6 capability was 27% and 43%. In North America, it was 51% and 55% in southern Asia (China being the main contributor).

3.2.2 Key Challenges

In this section, we describe some challenges IPv6 adoption must withstand. As we will see, many different factors are in play, making addressing these challenges a complex problem.

IPv6 comes with many improvements compared to IPv4. These improvements include a larger address space and security features such as *Stateless Address Auto Configuration*, *Internet Control Message Secure Neighbour Discovery*, confidentiality, encryption, and authentication support. The adoption of IPv6 has been a slow process and is still in its early stages. One of the main challenges to IPv6 adoption is the lack of global standardization for routing devices. Standardization is vital to the interoperability and scalability of IPv6 and plays a key role when convincing industrialists to use IPv6-enabled routing

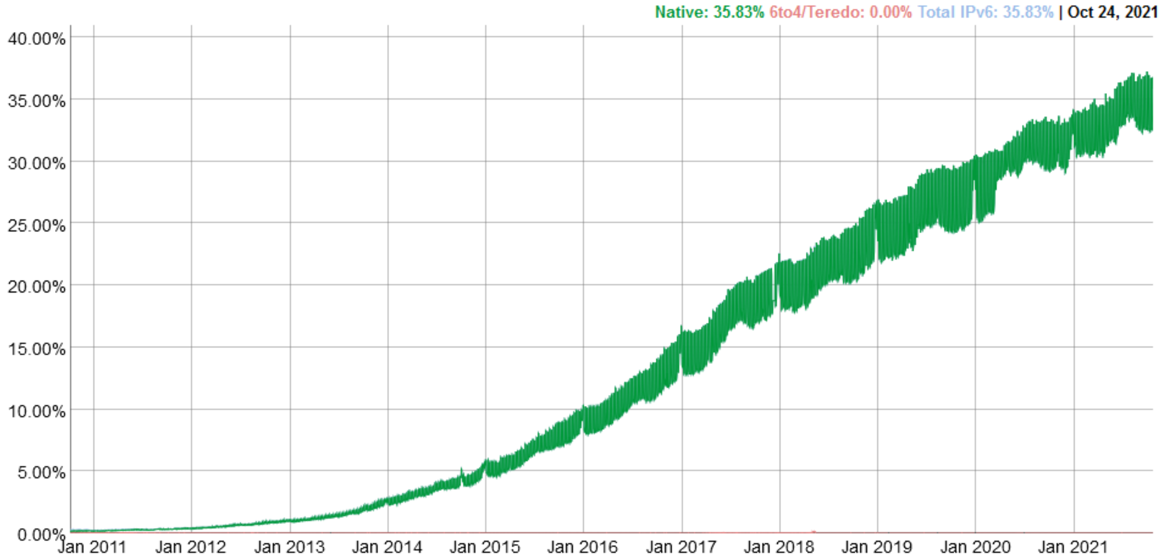

Figure3.1: Availability of IPv6 connectivity among Google users (24.10.2021)

mechanisms and technologies. Both IPv4 and IPv6 work stand-alone very proficiently for specific applications, but they don't collaborate for the newest routing requirements and latest application or technology trends.

IPv6 got standardized in 1998, but the adoption of the new standard did not gain speed until many years later. There were two main reasons why this was the case. Firstly, IPv4 and Ipv6 are incompatible and need an expensive infrastructure upgrade and transition techniques to allow IPv4 and IPv6 to coexist. Secondly, although IPv6 has many new features, these were not attractive enough to appeal to first adopters [31].

Australia had in 2018 an allocation of about 47.6 million IPv4 addresses while having a population of roughly 22 million people - approximately 2160 IPv4 addresses per 1000 citizens. In China, there are 1.3 billion people and 330.3 million IPv4 addresses. Meaning there are only 250 IPv4 addresses per 1000 citizens, making the need for transition to IPv6 a lot more urgent in China compared to Australia. The *China Next Generation Internet (CNGI)* project began in August 2003 as a five-year plan. The IPv6 adoption as part of the project. In 2014, reports state that Chinese carriers claimed to have implemented full IPv6 deployment. In Australia, few ISPs had, in 2016, fully implemented IPv6 or offered it to their customers. The differences show how the need for change is essential for IPv6 adoption.

A factor could be rooted in the five dimensions of national cultures (proposed by Hofstede). One of the dimensions is called individualism/collectivism. Australia is an individualistic society that focuses on individual achievement and productivity, while collectivist societies like China focus on group interest. The differences in culture could be a factor in how countries deal with IPv6 adoption differently. Individualistic societies would most likely try to emphasize how IPv6 can generate a competitive advantage - making the benefits of IPv6 compared to IPv4 less clear. The challenges of promoting IPv6 adoption could be rooted in focusing on the most suited aspects to different societies.

3.2.3 Transition Period

Tunneling enables one communication protocol to transmit another network protocol - a *virtual private network (VPN)* is an example of tunnel technology. While transitioning from IPv4 to IPv6, normal operations must not be affected. Tunneling technology can make the IPv6 packets transmit in the IPv4 network. Tunneling is useful when one of the communicators hasn't deployed IPv6.

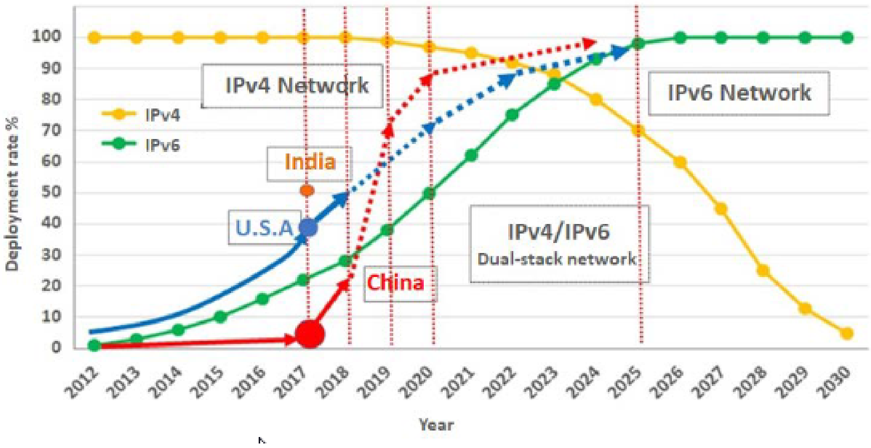

Figure3.2: IPv6 over IPv4 tunnel communication principle

In Figure 3.2, we see the basic principle for communication of IPv6 over IPv4 tunnel. As we can see, there will be a period where the IPv4/IPv6 dual-stack protocol unites the two protocols. An IPv4 header will be added to the IPv6 package when necessary before being forwarded to the IPv4 network for further routing. It is recommended to adopt the dual-stack technology and support (both) IPv4 and IPv6 to achieve optimal transformation. Dual-stack technology will help the gradual evolution to a pure IPv6 environment.

3.3 Moving to an IPv6-based future IoT

The function of one individual connected device may be enhanced by connecting it to related products. A light bulb can be connected to other light bulbs and create easily configurable lights in the living room. The fridge could be connected to your phone and give alerts when some products are going bad, or you're soon all out of milk. The *Internet of Things (IoT)* is defined by "the networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the Internet" [32]. IoT has become a market with substantial growth over the past years and has quickly become a household name, especially after the emergence of "smart" homes. IoT was first coined by Kevin Ashton in 1999 with reference to supply chain management. The IoT concept revolves around its "smartness" in obtaining knowledge and applying it. The ultimate goal of IoT is "to plug and play smart objects". In this section, we will look at what impact IoT will have on IPv6, and how IPv6 will help to enable the use of IoT.

3.3.1 What is IoT6?

The amount of IoT devices has surpassed the number of human beings connected - leading to IPv4 address space being exhausted. The approximately 4 billion address space of IPv4 reached its limit on the 3rd of Feb 2011 at the global level. IPv6 is scaling up and creating an almost unlimited number of globally reachable addresses. IoT6 is a European research project on the Internet of Things aiming at exploiting the potential of IPv6 to address the current needs of IoT. The outcome of IoT6 is recommendations on IPv6 features for the Internet of Things and an open and well-defined IPv6-based Service-Oriented Architecture [33].

3.3.2 IoT6 Architecture

IoT has had many different specified architectures over the years. However, many of them use the requirements of their specific project. This limitation has made the approaches to IoT architecture various, and each architecture often utilizes different components and protocols. There have been significant efforts attempting to define a universal architecture for IoT, like the IoT-A and IoT-I projects. The IoT6 project aims at creating a scalable *Service Oriented Architecture (SOA)* based on IPv6 to achieve interoperability between different communication technologies and interaction with application-based services. The decision was to utilize the embedded IPv6 features to enable functions currently implemented using higher layer protocols.

IoT consists of three components that form the basis for its architecture:

1. *Hardware* - Comprises sensor nodes, their embedded communication, and interfacing circuitry.
2. *Middleware* - Comprises data storage, analysis, and handling resources.
3. *Presentation layer* - Comprises efficient visualization tools compatible with different platforms for different applications. It presents the data to the end-user in an understandable form.

Many parameters affect the architecture of IoT, and therefore many research efforts try to create an optimized architecture that addresses issues like scalability, security, addressability, and efficient energy use. To solve the problem of scalability, researchers are developing various multi-hop routing protocols covering a larger area and are self-adapting. Device-efficient MAC protocols, energy harvesting techniques, and cross-layer protocols could solve the energy consumption issue. [34] suggests using a combination of IPv6 for address space and 6LoWPAN for integration of low-power IEEE 802.15.4 devices.

3.3.3 IPv6 and IoT

The number of connected devices has now surpassed the number of interconnected humans and will grow far past the human population. Reports from Ericsson state that 28 billion “smart” devices will be connected across the world by 2021 [35]. IPv4 has been the most used protocol for the network layer in the last decades, but the protocol is not designed for IoT. *Internet Assigned Numbers Authority (IANA)* and the RIRs adopted IPv6 to replace IPv4 as IPv6 answers to IPv4’s limitations, especially that of address space. There has also been an emergence of standards specifically designed for IoT that has enabled highly constrained devices to become (natively) IP compliant. Some examples of such protocols are 6LoWPAN, CoAP, and CoRE. The specifics of these protocols are beyond the scope of this article.

3.3.4 IoT Forecast

The future will involve “smart” homes of connected devices that send information when necessary, “smart” cities that change the management of traffic, pollution, and disasters. The quality of healthcare services will improve - doctors can monitor patients in real-time and provide treatments remotely. Energy management will become more efficient when “smart home” devices such as air-conditioners, refrigerators, and washing machines communicate and react to specific scenarios.

IoT is a fast-growing market and will play a crucial role in the future of consumers and businesses. IoT can increase profits for any organization and make life easier for people. A report from *National Advances IPv6 Center (NAv6)* looks at the growth of IoT and tries to predict the further development of the market [36]. The global IoT market is forecasted to grow with a *compound annual growth rate (CAGR)* of 39% from the year 2020 to 2030, going from 245 billion US dollars to 8 131 billion US dollars. The retail sector projects a CAGR of 84%, and the energy and utility sector projects a CAGR of 62%.

3.4 5G and IPv6

The 5G standard is a work in progress and refers to the fifth generation of cellular mobile communication. 5G, like IPv6, is not backward compatible and is therefore required for all new hardware and software [37]. IPv6 becoming native will take time. The introduction of new technologies (such as 5G) could play a vital role in furthering the adoption of IPv6.

The 5G world will move to IPv6-Only as announced by some early adopters such as T-Mobile. Mobile Network Operators (MNOs) that need larger address space will also find it challenging to get enough IPv4 addresses. *Reliance Jio* in India deployed 4G with IPv6-Only and has approximately 250 million IPv6 users - 91.06% of their traffic is now measured to be through IPv6.

Both IoT and 5G could be important factors to the ongoing push for the full adoption of IPv6 and switching from IPv4. Wireless technologies like 1G, 2G, 2.5G, 3G, 3.5G, and 4G are not optimized for IoT devices that require low power and less data rate. We can therefore expect a shift towards 5G. “Smart” city applications such as “smart” energy, “smart” security, “smart” transport, “smart” health, and others will be a reality in 5G networks. 5G addresses the main challenges more effectively compared to its predecessors. These challenges are:

- Large bandwidth
- Higher data-rate
- Massive connectivity
- Low end-to-end latency
- Cost-effectiveness

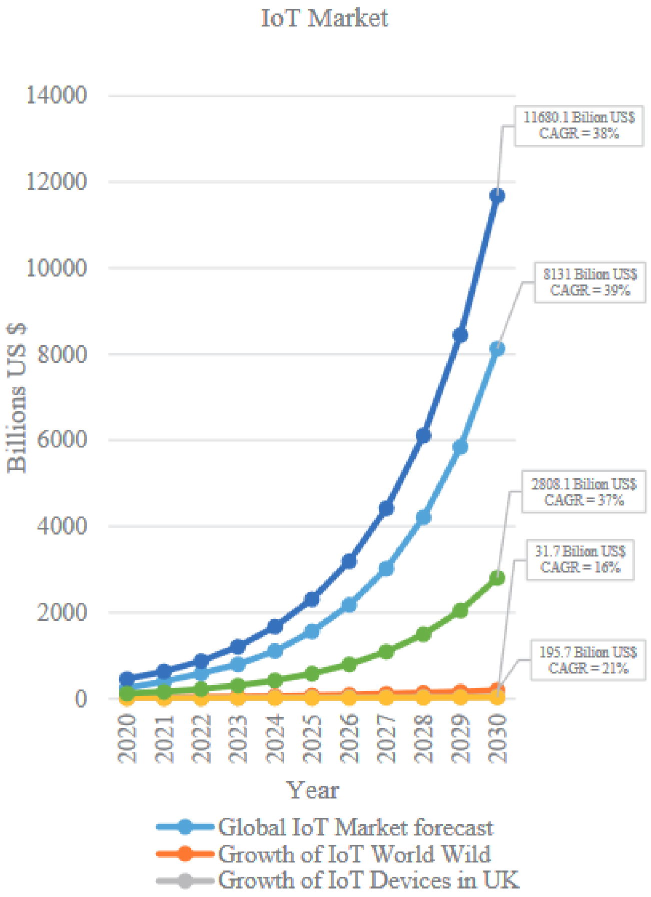

Figure3.3: IoT Market in Billions US $ - (2020-2030)

- Consistent Quality of Service (QoS)
- Device computational capabilities
- Device intelligence services

For 5G networks to meet QoS requirements, devices running IPv6 needs to communicate efficiently with devices running IPv4. Three technologies have been suggested to meet this demand; *dual stack*, *tunneling* and *translation*. With dual-stack, the devices on the network have inbuilt support for both IPv4 and IPv6. The devices usually give preference to IPv6. Dual-stack creates a more complex environment than IPv4-only or IPv6-only networks. Tunneling allows private network data to transmit over a public network. The technology ensures transmitted data are inaccessible by nodes in the public network. The technology will be useful to ensure reliable IP addressing in the transition towards IPv6-only next-generation networks. After the 5G-network deployment, more devices will be running IPv6 rather than IPv4. Therefore, it will be suitable to run IPv4 over IPv6 networks for simplicity. Translation from IPv4 to IPv6 is different from IPv4 NAT. IPv6 and IPv4 have different structures and are incompatible, making the translation process more complex. Nevertheless, translation is preferable to dual-stack and tunneling because of the following reasons [38];

- Translation is seamless and gradual when migrating from IPv4 to IPv6.
- In 5G networks, service providers can provide services transparently to IPv4 Internet users.

3.5 Summary/Conclusion

The adoption of IPv6 has become essential to the next-generation networks. IoT is a rapidly growing market and making an important impact on the address space. In the future, more devices will connect than ever before. To utilize these devices effectively, factors like Quality of Service (QoS), security, and scalability. These are factors that IPv6 tries to address. However, the transition to IPv6-only is a slow process. This process requires new technologies with solutions to the incompatibility between IPv4 and IPv6.

Incompatibility is one of the reasons why the adoption has taken such a long time - especially the slow start. On the contrary, new technologies like IoT and 5G will boost the IPv6 deployment process. These technologies are dependent on vast address space and will make the need for transition a lot more imminent. China and India have seen this necessity for a long time (because of their large population) and were early to start extensive projects to meet this demand. Countries that didn't, like Australia, will now find themself behind in modern development, relying more on transition technologies.

The pace of adoption has been slow, but statistics show that the speed is accelerating, and the use of IPv6 is becoming more and more common. IPv4 is no longer sustainable for the requirements of present and future networking. IPv6 is designed for the future and will hopefully fill the needs of the ever-growing Internet far into the foreseeable future.

CHAPTER

FOUR

AN OVERVIEW OF 5G AND ITS SERVICES

Abstract

The meaning of this paper is to elaborate on 5G's design and architecture, its provided services and security architecture. The questions to be answered is how the network for this upcoming technology is implemented by the mobile network operators and how the next generation network infrastructure looks like when established. 5G stands for "fifth generation" and it's going to be the fifth standard for mobile wireless network [39]. 5G will surpass the previous technology, but it will probably compliment 4G for mobile users and devices connecting to a wireless network for the next decade or more. Regular call between persons will still likely be managed by the 4G network for a period in the future [40]. Data transfer is highly likely to be managed by 5G. Not only for traditional mobile phones, but also for wireless home connection to internet instead of cabled access where its reasonable.

This paper will in the start give an overview of the technology, before it will elaborate on the implementation's status, the difference from previous standard, and the design and architecture. The paper will end up with presenting some of the possibilities that lays in this next generation network and which security features that are implemented, before its end with a conclusion of where the technology is today.

4.1 Overview of the 5G technology

The background for development of 5G has its outcome from the increase in the total number of mobile users and the demand for more data rises. 5G must handle more traffic at a much higher speed then today's cellular network, it must be more reliable and support lower latency than previous standards. The 3rd Generation Partnership Project (3GPP) is an umbrella organization for several other standards organization created for developing protocols for mobile telecommunication [41]. They are the organization who has defined the global specification for the 5G technology. And it's the organization that governed the standard. It's possible to connect non-3GPP 5G network with an 3GPP network because of standardization of connection sockets. There is not one specific company or person developing 5G. It's several companies contributing to the realization of 5G.

5G will most likely be the foundation of Virtual reality (VR), autonomous driving, Internet of things and stuff we cannot yet even imagine, for example like remote surgery.

4.2 Implementation's status

The implementation of 5G started with the phone companies deploying the technology in 2019. GSMA as a global organization managing the interest of the mobile network operators has through own studies forecasted the total of 5G connection to surpass 1.8 billion in 2025 [42]. This will leave the 5G technology up to 21 percent of the total connections, with U.S and developed Asian countries in the lead. Her in Norway both Telenor and Telia as the two biggest mobile service providers have started establishing 5G network in the biggest cities and are planning to cover the entire country in respectively year 2023 and 2024 [43, 44]. In total there was 224 operators in April 2018 that were investing in 5G technology [45]. These operators divided in to 88 countries are investing to perform test, trials, pilots or planned or actual deployments. At the same time 39 operators had announced that they had deployed either 3GPP-compliant or non 3GPP-compliant 5G technology in their respective network as a part of upgrading for supporting more connections and higher data transfer.

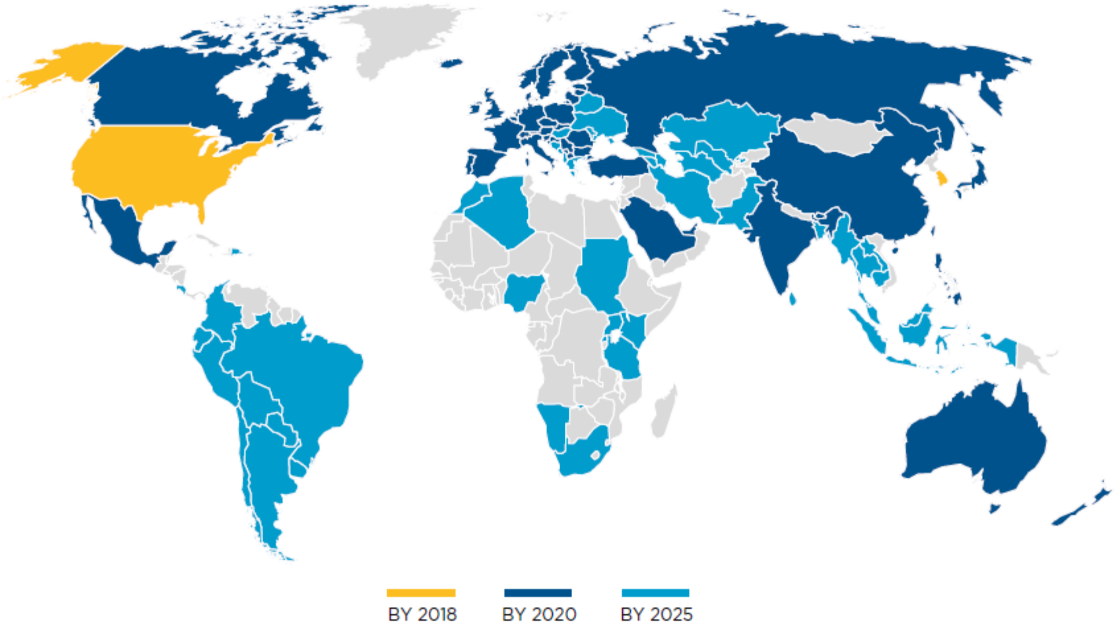

Figure4.1: 5G launches plans and projects per country. [40]

4.3 Differences from today's technology

5G technology is developed from several stakeholders since 2012 to define what 5G should become. And in 2015 the International Telecommunications Union Radiocommunications Sector (ITU-R) presented the requirements for the 5G design goals [40]. This have made the foundation of what 5G has become today. Requirements for data rate were set to a peak of 20Gb/s downlink and 10Gb/s for uplink. Latency on the user plane were suppose to become much lower than 4G and end up in between 1ms to 4 ms. The connection density could be as high as up to 1,000,000 per km.

This is making 5G from 10-times and up to 100-times faster than we are familiar with data transfer today. The latency will be around 10-times smaller in 5G compared to 4G's 20 ms. This is because of the use of more advanced core network and several changes in spectral use. This new network will probably support from 10- to 100-times more connected devices making it suitable for the increase of wireless devices. 5G will probably also have 1000-times more capacity in data transfer, reduced energy consumption, and are assumed to have an availability up to 99,999% [40].

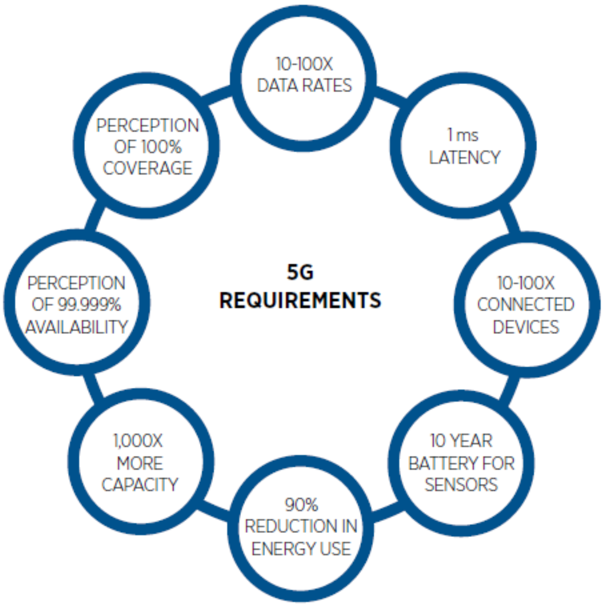
5G REQUIREMENTS
10-100X DATA RATES
1 ms LATENCY
10-100X CONNECTED DEVICES
10 YEAR BATTERY FOR SENSORS
90% REDUCTION IN ENERGY USE
1,000X MORE CAPACITY
PERCEPTION OF 99.999% AVAILABILITY
PERCEPTION OF 100% COVERAGE

Figure4.2: The 5G comparisons with 4G. [40]

4.4 Design and architecture

So how is the 5G technology achieving its faster data and more reliable services. Which technologies are making this possible? We will now run through an overview [46] from the Institute of Electrical and Electronics Engineers (IEEE) who is an ideal organization consisting of professionals in electronics and electrical engineering.

Millimeter waves is one of the fundamental technology improvements for making 5G ready for more mobile user and faster data speed. Until today, mobile technology has used almost the same radiofrequency spectrum [46]. But with the increase of devices the limitation of the radio spectrum is causing less bandwidth for everyone. Less bandwidth is again making services slower and causing more dropped connections. The millimeter waves are frequencies in the band of 30 to 300 gigahertz. They have not been used for transmitting data for mobile user before. With the implementation of this frequencies the mobile network can utilize higher data bandwidth because of their abilities to transport more data. The drawback of millimeter waves is their lack of ability to travel through obstacles like walls in urban environment and terrain obstacle for coverage at a distance.

To mitigation the drawback of using millimeter waves the 5G network will use "small cells" to supplement the traditional base station for cellular network. Small cells are small tower mini base-stations used to prevent the problem with frequencies stopping at obstacles. Their purpose is relaying signal to the data user who doesn't have line of sight to the traditional base station. They are smaller because of only transmitting tiny millimeter waves and can be placed more easily around on existing infrastructure in the urban environment. Because of the shorter transmitting range frequencies can be reused by other stations in different areas making the use more efficient. The drawback for needing a higher number of small cells is the difficultly of making a proper coverage in rural areas.

The increase in total of devices on the mobile network means that the base station needs to handle more connections. This is planned to be solved in 5G with the massive MIMO (Multiple input, multiple output) technology. 4G base stations has a dozen ports for antennas and 5G will have up to a hundred ports. This meaning many more users can connect and send data at the same time. This is supposed to increase the capacity by a factor of 22 or more [39]. More antennas, sending more signal also means the possibility for interferences when signal crosses which are increasing with massive MIMO.

Beamforming is another feature implemented to prevent the interferences problem mentioned above. The idea is to focus the stream of data to a specific user and not broadcasting the data to everyone like it's done today. This is supposed to be way more efficient. Base station can handle more data at once because of the advanced algorithms plotting the best direction for transmission. They can even calculate the use of bouncing on walls before arriving at destination making interference less relevant. Another positive effect of beamforming is the ability to direct all data transmitting effect in one direction and not 360 degrees like 4G. This is making the signal travel longer reducing the negative effect of shorter transmitting range by using millimeter waves. The signal is more intact and will reduce the use of channel coding techniques for protecting the signal from noise and interference. For 5G low-density parity-check (LDPC) is chosen because of its ability to support higher throughput and reliability, and its support for incremental-redundancy that reduce the size of encoding and decoding when the data rate is high [47].

Today's transceivers used in wireless mobile network are develop for either taking turn in sending and receiving data, or to use more than one frequency to achieve full duplex [46]. In 5G technology full duplex on the same frequency is being implemented to double the capacity for transmitting and receiving data. It has been assembled silicon transistor solving this possible problem already. The difficulties about full duplex are to prevent the interference being created when a transmitter emits a signal that is much stronger than the received signal. This reveals the need for special echo-cancelling technology in 5G for receiving and transmitting at the same time.

These five different technologies are now being used to build the future network for wireless connection. It likely will make throughput, reliability, and low latency better in 5G than the previous standards. It will also be a more unified platform who is more capable than 4G and uses the frequency spectrum better.

4.5 Services provided in 5G

When listening to commercial from mobile network providers, they focus a lot of not only the increase of data transfer speed with 5G. One Norwegian commercial has a saying that goes like “10-times faster, 1000 more possibilities”. All these possibilities we are not even able to imagine yet but is highly likely that 5G will bring the future closer to use.

5G is used across three types of connected services seen from a broad perspective. These are enhanced mobile broadband (eMBB), mission critical communication and massive IoT [48].

The eMBB is one of the earliest use-case for the development of 5G. The aim is to provide broadband services directly to customers all around the globe [40]. eMBB will support the user with the possibility of doing any internet-based activity wireless on a mobile device. This is possible through the higher data transmit rate and lower latency. Use of any types of videos is saturating in today’s wireless network. 5G will support video performances at a better quality. It’s possible that 5G will be able to support immersive experiences like virtual reality (VR) and augmented reality (AR) with faster, more uniform data rates, lower latency, and lower cost-per-bit soon.

A by-product of excess eMBB capacity is Fixed Wireless Access (FWA). This is enabling mobile operators the possibilities to make solution for known and new broadband opportunities [40]. FWA is not a new idea but have been more relevant when 5G with eMBB is deployed. There are four known use cases for FWA. The two first use cases are broadband for the unconnected and in competition with fixed broadband. This is the possibilities to provide wireless broadband through 5G for home connection or in business premises. The best opportunity to enter this new market for mobile operators are premises that have not been connected earlier or is connected with legacy cooper or DSL broadband instead of connection through fiber. This is an opportunity to provide broadband connectivity to rural and suburban premises with a cost economic alternative compared to fixed fiber. 5G FWA for replacing fixed fiber is a more polarizing proposition. This is something that is unproven and only the future will tell if 5G broadband is competitive in regard of speed, performances, and price.

The third use case for FWA is backup broadband. The use is related to the need of stable and reliable internet connection for businesses as they are increasing and the need for backup solution being more important. A backup broadband could ensure little downtime and thereby keeping production up. The last use case for FWA is backhauled connection for 5G small cells. With the advanced beamforming mobile base stations may not need to have a fixed fiber connection for backhaul. 5G backhaul could be more cost-economic to use.

The second type of connected services is mission-critical communications. 5G will have with its ultra-reliable, available, low latency links the possibilities to support with new services that can transform the industries. It has already been presented use cases for this type of connections and remote control of critical infrastructure, vehicle and medical procedures is likely to be made possible using 5G. The Fourth Industrial Revolution (Industry 4.0) is an example of where mission-critical communications most likely will be needed. Industry 4.0 is the ongoing increase of automation with the use of machine-to-machine (M2M) and IoT deployed in the traditional manufacturing [50]. With the ability for the machines to analyze and communicate to each other, the need for reliable communication solution increases. Deploying of sensor could be done in new reachable places where cabled solution for communication is not an alternative, but a wireless 5G possibility is. Real-time control is another use that is important when automate manufacturing processes. Being able to follow production live

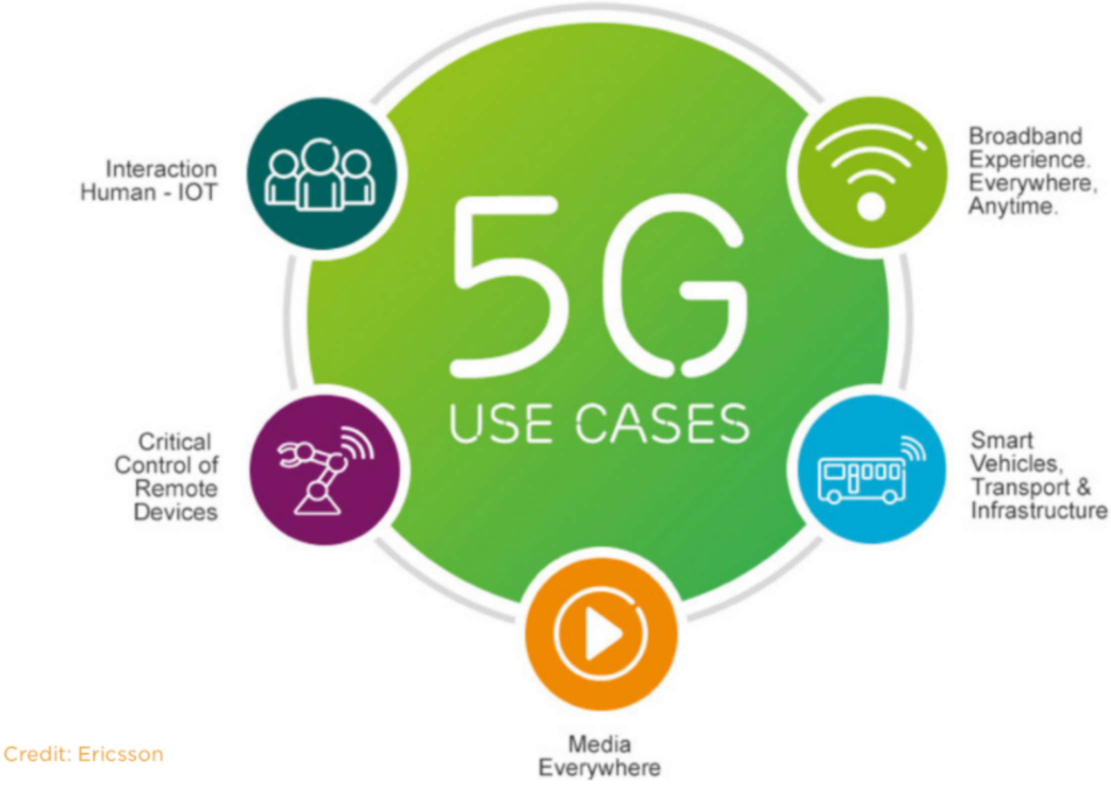

Figure4.3: Different use case for 5G technology. [49]

is very useful. We probably will also stop some of the mass producing because of machines being smarter and can produce customize products without delay in production line. GSMA define Industry 4.0 as the biggest geopolitical driver for 5G [40].

Critical infrastructure like emergency services, power supply, waste and water, electronical payment and more could utilize 5G technology in regard of mission-critical communication. There is a lot of examples of 4G in use for that purpose already today and 5G will probably give even more possibilities. 4G is already in use for public safety networks in UK, US, and South Korea [51]. They already have a push to talk (PTT) use in combination of TETRA and LTE for public safety. 5G with its eMBB and ultra-reliable and low latency communication (URLLC) could be useful for example in even lager real time live video streaming integrated with massive IoT sensors for operators in operation room to surveille the safety for public-safety worker. Another example could be new usage of massive IoT sensors for detecting gunshots and dangerous chemicals deployed in places where needed. The data speed presented by eMBB could possibly be used for a combination of Artificial Intelligence (AI) and real time video for intelligent surveillance with less human resources doing the work [51].

Other use cases are in agriculture were the use of massive sensor and autonomous vehicle could lead to more precision harvesting of the fields with less human resources. Sensors could detect pets in field, or pest and diseases in the crops.

Cellular Vehicle-to-everything (C-V2X) technology is also standardized by 3GPP and it’s a part of the roadmap to 5G connectivity [52]. This technology can in cooperation with 5G change the way of driving in the future and making the road safety better. This technology could provide queue warning, collision avoiding, warning of hazards ahead, collecting road tolls, increase autonomous driving and more. With 5G and its low latency, vehicle and traffic infrastructure like traffic lights could communicate together more extensively. And maybe communication between vehicle and cyclist for collision avoiding could be possible.

eHealth is also assumed to a be part of mission-critical communication. This could be used for example in the health services for surveillance of sick people’s health. The military could also us the same technology for alerting if abnormal states of dehydration and heart rate in combat zones. And the data could be forwarded to a medical response team.

A lot of the examples from mission-critical communication is in the category of critical IoT which is in short anything that is requiring a constant data connection to be functional. 5G with its supporting enhanced quality of services and low latency is needed for full effect and thereby to give the needed reliability. Massive IOT is the third and last type of connected services for the 5G technology. Unlike critical IOT, massive IoT is driven by scale rather than speed [53]. In the design of 5G it’s meant to support seamlessly connection of a massive number of embedded sensors. These sensors could be places in virtually everything and 5G were to support these with the ability to scale down in data rates, power, and mobility. This ends up with an extremely lean and low-cost connectivity solutions for massive IoT. Already a lot of device comes with integrated eSIM for connectivity without bringing your cellular phone. For example, we already se watches and headsets have eSIM integrated. In the future it also probably will include device from medical equipment’s to entire factories. With the support of connectivity for about one million devices per square kilometer to the 5G network this usage is supported in the future.

Enhanced network slicing is a feature under development for the 5G technology. In short, it’s the use of network virtualization to divide a single network connection into several distinct virtual connections.

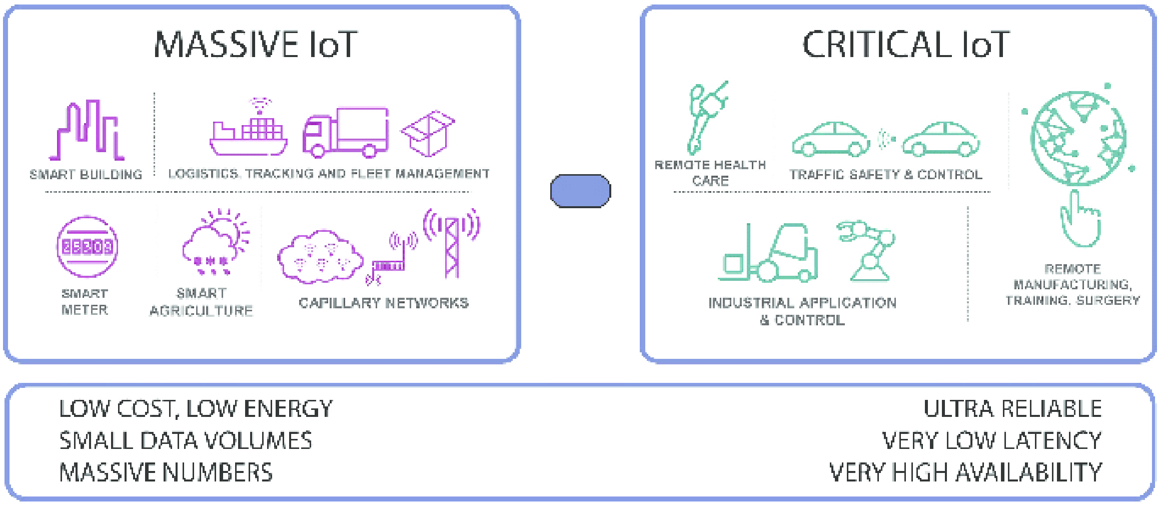

Figure4.4: Massive IoT vs. Critical IoT. [54]

The aim for dividing is to be able to provide different amounts of resources like speed and latency for different type of traffic. This architecture leverage of the principles of network functions virtualization (NFV) and software defined network (SDN) that is implemented in the 5G radio technology [55]. This is giving a flexible, programmable network where traffic can be divided in different slices. Each network slice is then isolated and work like end-to-end network within the one original single network. Inside these networks slice the mobile operators could sell guaranteed throughput and low latency for one specific service. Samsung has explored this technology and has discussed a hospital network as an example for network slicing. It could be prioritized bandwidth for emergency room admission, and less to services that being provided for visitors [56].

4.6 Security features implemented

Many of the implemented security features in 5G has its outcome from the previous standardizations in telecommunication. Security mechanisms provided by 3GPP for the 5G standard therefore include previous implementations from 4G, but also include new measurements like encryption, authentication, and user privacy [57].

Some of the most important security enhancements is described in 3GPP standards [57]. First up is the possibility for mutual authentication. This provides authentication for both the end user and the network for providing enhanced security. The end user is being authenticate for being able to access the mobile network, but also accountability to keep control of which user is linked to which IP and when. Authentication also provide the possibility to lawful intercept for keeping the 5G network secure. To ensure the end user, the network is also authenticated towards him for stating they are connected to a legitimate network.

The confidentiality of user data is provided through encryption in 5G. All user data is encrypted when pushed out on the mobile network to prevent eavesdropping. The data is only protected by the 3GPP standardization when its on the mobile network. Traversing to Internet there need to be other security measures to encrypt the data traffic. The next security feature is privacy for the end user to protect user identifier. This feature is also only protected inside the 5G network. To be protected on Internet or destination server the application provider itself must ensure end to end confidentiality.

The 3GPP standardize the use of encryption and integrity protection algorithms to provide reliability and robustness in the mobile network. The goal is to prevent problems when bad links or radio connections occur from non-malicious unavailability situations. Also, previous problem with false base station in GSM is more evolved in the 5G technology then previous standardization. Problems with false base station receiving and identifying the user through the IMSI (International Mobile Subscriber Identity) is prevented because of not transmitting the user's long-term identifier in clear text. 5G also improves the security by changing the temporary user identifiers increasingly from earlier generation mobile network.

The last in security feature elaborated by Ericsson is compartmentalization [57]. The purpose of compartmentalization is to reduce the impact on e.g., security breaches by dividing the network structure in smaller compartments. This aims to reduce the problem escalation from one part to another inside the network. An example of this, is the split between the radio access network and the core network functions in 5G. Unauthorized access to the radio network will not compromise data in the core network.

4.7 Security policies

Security risk and threats requires implementation of security policies and several security controls to mitigate the potential impact. Since the mobile network have become more and more important and its even being classified as a critical infrastructure some places, 3GPP and GSMA toke the initiative to create a security assurance scheme. This scheme is called the Network Equipment Security Assurances Scheme (NESAS) [57]. NESAS consist of two different element which are security requirements and auditing infrastructure. 3GPP defines the requirements and they are collected in so called Security Assurance Specification (SCAS). Examples of requirements is, defining security requirements for 5G base stations, functional security policies such as minimum length of management password, qualitive requirements for hardening and penetration testing for a mobile network operator, and much more.

GSMA handle the auditing infrastructure for its member by appointing audit firms. The purpose is to perform audit of mobile network operators' development and testing processes. GSMA awards certificates to mobile network operators passing the auditing process. This is engaging vendors to prioritize own security to protect customers data and preventing expensive recovery after cyber-attacks towards their network. NESAS is aiming to meet the claim of both national and international cybersecurity regulations in their work. The NESAS scheme should be used as a globally common baseline for providing security assurance [58] and other mechanism should be used alongside for enhanced protection. This could be the individual operators or national IT security agencies that want to put additional security requirements to cover the entire lifecycle of a network.

4.8 Conclusion

Implementation of 5G standard throughout the entire world is increasing rapidly to meet the demand for wireless connection everywhere. The technology is introducing new features along with the implementation that will introduce new possibilities. Both enhanced mobile broadband (eMBB), mission critical communication and massive IoT is technology with existing use cases that will change how communication is being completed in near future. As always, new technology introduces new security risks and future challenges for the mobile operators to handle. Meeting this data security concerns will be important because in the future we will probably see more aggressive attacks when malicious actors are testing the vulnerabilities. Especially in the growing of IoT networks. For customers investing in IoT solutions, data security will probably become a competitive differentiator [53].

When more use cases for 5G arise, more opportunities for invasion of privacy will occur. Physical harm and theft of data will increase, like it has been in previous years. Mobile network operators must handle this problem in coordination's with national and international security organization. The work done by organizations like 3GPP and GSMA will be more crucial in the future and the importance could not be underestimated. The 5G standard will highly likely be a socially changing technology if the security risk is handled in a proper manner.

CHAPTER

FIVE

INTRODUCTION TO LORA TECHNOLOGY

5.1 Introduction to LoRa

This paper will deal with the communication technology LoRa, how the technology is built up and how it works in relation to other wireless technology, as well as a review of the security of the technology.

LoRa is an emerging technology that is becoming more and more relevant as internet of things (IoT) becomes more widespread.

LoRa stands for Long Range and is a technology for wireless transmission of data over long distances, with low energy consumption. LoRa was developed by Cycleo, a French company, before Cycleo and its technologies was acquired by Semtech Corporation. LoRa is the name of the radio technology and is a wireless transmission solution in the physical layer of the network stack. To be able to implement the communication technology, different protocols in the networking layer are invented, one of these protocols is LoRaWAN. LoRaWAN is an abbreviation for Long Range Wide Area Network and is a registered trademark of Semtech, but today the specification is developed and maintained by the LoRa Alliance.

The LoRa Alliance describes the LoRaWAN specification as “a Low Power, Wide Area (LPWA) networking protocol designed to wirelessly connect battery operated ‘things’ to the internet in regional, national or global networks, and targets key Internet of Things (IoT) requirements such as bi-directional communication, end-to-end security, mobility and localization services” [59].

Because LoRa and LoRaWAN are so tightly integrated, and because the vast majority of sources that discuss the technology focus on LoRaWAN, this paper will largely deal with both LoRa and LoRaWAN where this is relevant.

5.2 LoRa as part of wireless technologies

LoRaWAN are part of a larger family of technologies known as LPWAN (Low Power Wide Area Networking). Semtech refers to LoRa as the de facto wireless platform of Internet of Things (IoT) [60], but other IoT network technologies such as Narrowband-IoT (NB-IoT) and Long-Term Evolution for Machine (LTE-M) are implemented by major mobile operators [61].

Devices with LPWANs technology can connect over distances up to 24 kilometers and at the same time deliver battery life of up to 10 years. The three most important characteristics of an IoT network are low cost, low power consumption and good security [62].

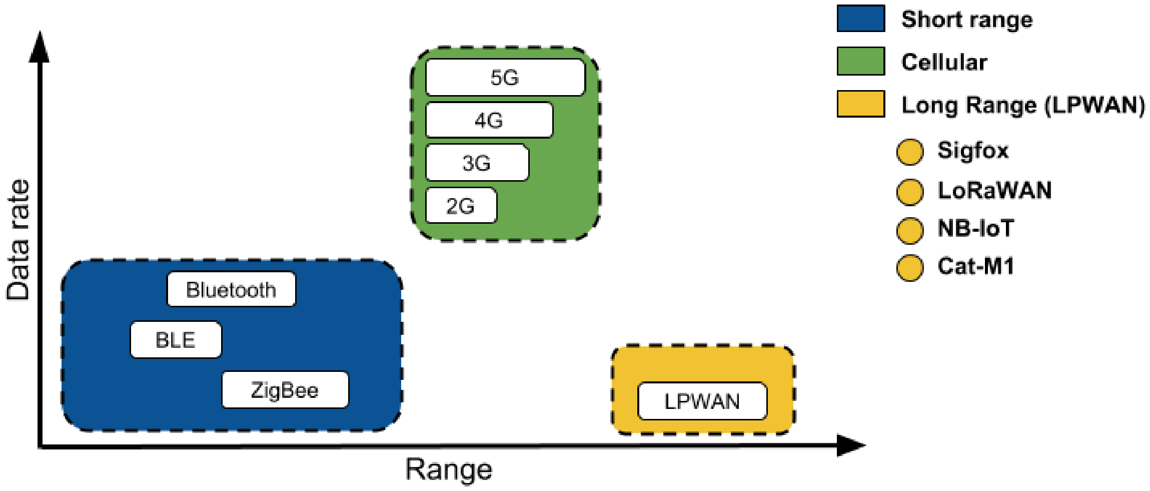

Figure5.1: LoRaWAN as part of LPWAN in relation to wireless and mobile technologies [63]

Figure 5.1 shows LoRaWAN as part of LPWAN in relation to wireless and mobile technologies. The LPWAN technologies, Sigfox, NB-IoT and Cat-M1, listed in this diagram, is together with LTE-M the biggest competitors to LoRaWAN. Sigfox is the technology with the biggest similarities with LoRaWAN, with long battery-life, cost efficiency, high range, and easy deployment. NB-IoT and Cat-M1 have better latency performance, payload size and scalability [63].

The technologies that Norwegian telecom operators seem to prefer and prioritize for their IoT networks are NB-IoT and LTE-M. Telia does not mention any of the other NPWAN technologies, but it may appear that Telenor does not want to invest in other technologies such as LoRaWAN due to lower security [61, 64].

5.3 The technology behind LoRa and LoRaWAN

As shown in Figure 5.1, 5G and LPWAN technologies such as LoRaWAN belongs to different segments of wireless and mobile communication technologies, nevertheless, some believe that 5G and LoRaWAN will be closely integrated in the future. It can be stated that 5G and LoRaWAN will in the future complement each other in that 5G can be used as a network infrastructure for the traffic between the gateways in LoRaWAN and the remaining infrastructure [66].

Conversely, LoRaWAN can complement 5G, by being a communication technology in IoT networks primarily based on 5G, where IoT devices that are to communicate over greater distances with low energy consumption use LoRaWAN. Because LoRaWAN is a technology that can solve tasks where 5G is not ideal, LoRaWAN is described as a technology that can close the gap for applications where low power consumption, long range and the ability to penetrate physical structures are required [60, 65].

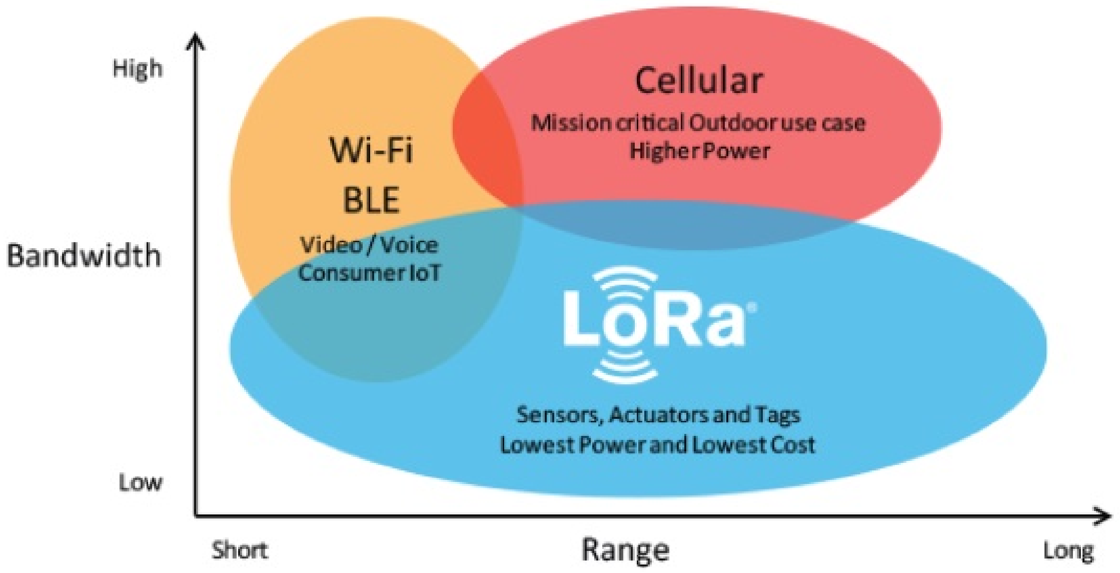
High
Bandwidth
Low
Wi-Fi
BLE
Video / Voice
Consumer IoT
Cellular
Mission critical Outdoor use case
Higher Power
LoRa
Sensors, Actuators and Tags
Lowest Power and Lowest Cost
Short
Range
Long

Figure5.2: LoRa in relation to wireless and cellular technologies [65]

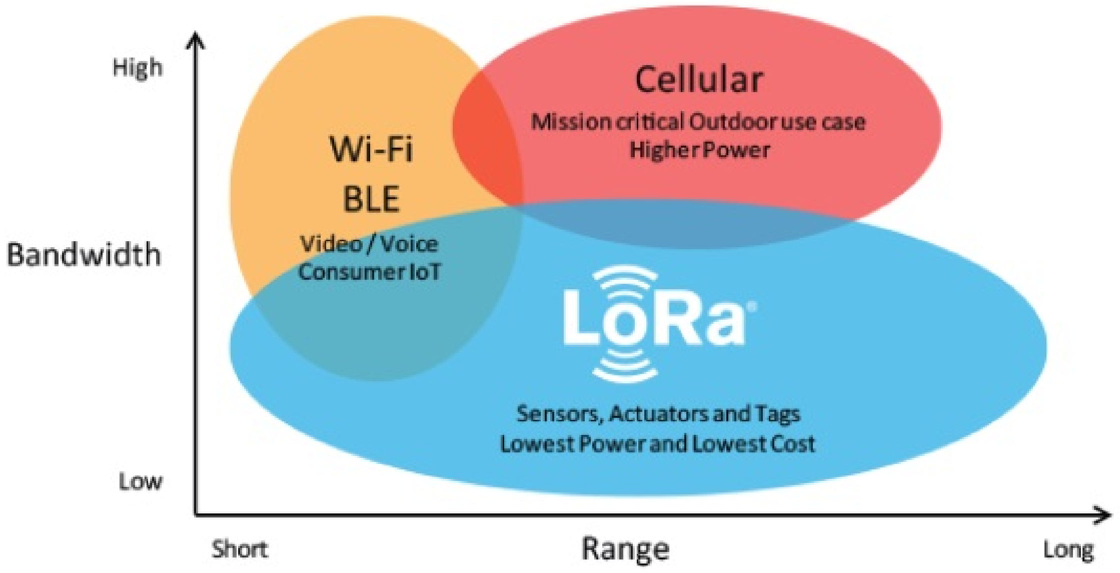
High
Bandwidth
Low
Wi-Fi
BLE
Video / Voice
Consumer IoT
Cellular
Mission critical Outdoor use case
Higher Power
LoRa
Sensors, Actuators and Tags
Lowest Power and Lowest Cost
Short
Range
Long

Figure5.3: LoRaWAN Network Arctitecture [65]

5.4 Security in LoRa and LoRaWAN

To assess the security of LoRa it is necessary to distinguish between LoRa and LoRaWAN as this is the implementation of the technology in two different layers of the network stack As Lora is the wireless transmission solution in the physical layer of the network stack.

As previously mentioned LoRa is the wireless transmission solution in the physical layer of the network stack, it is not clear from sources what security is implemented at this layer, as it is largely mentioned in connection with LoRaWAN. Semtech itself states LoRa as secure with features such as “end-to-end AES128 encryption, mutual authentication, integrity protection, and confidentiality”, but this type of security is normally implemented at higher levels of the network stack. The security features that Semtech states are also the same as the LoRa alliance refers to in its review of the security of LoRaWAN, it is therefore probable that the security Semtech aims at is not actually implemented in LoRa, but in LoRaWAN.

The physical layer of LoRa has in any case a certain degree of security built in, as LoRa is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology. Chirp spread spectrum was originally developed for military applications to help ensure secure and reliable communication and is a long-range radio-frequency technology that’s very difficult to detect and intercept when operating at low power [67].

According to the LoRa alliance LoRaWANs security is designed to fit the general purpose and design of the networking protocol. This includes low power consumption, low implementation complexity, low cost, and high scalability [68]. This can be interpreted in different ways, either in that the security of the protocol is as good as possible for such a technology, or in that the security has been set aside to achieve other properties of the protocol.

The lora alliance’s primary selling point for LoRaWAN security is end-to-end encryption, which they achieve with a 128-bit AES application session key [69].

In addition to AES encryption, the alliance states that LoRaWAN uses “CMAC2 for integrity protection and CTR3 for encryption. Each LoRaWAN device is personalized with a unique 128-bit AES key (called AppKey) and a globally unique identifier (EUI-64-based DevEUI), both of which are used during the device authentication process” [68].

Although Semtech and the LoRa alliance talk warmly about the security of LoRaWAN, there are several sources online that criticize their security. Telenor, one of the leading telecom operators in Norway, refers to LoRaWAN as a “network technology thats relevant for services that do not have as high security requirements. Typical applications are measurement of water temperature or air quality” [61]. This assessment gives LoRaWAN a limited application and does not front LoRaWAN as the leading IoT technology. IoT providers like Ubidots describe LoRaWAN security as weaker than their competitors. In a blog post where they compare the technologies, LoRaWAN is referred to as “a low power IoT protocol that comprises the LoRa radio technology, allowing for an open, reliable, and economical network deployment. By contrast, NB-IoT is a licensed LTE radio technology offering low latency and strong security at a steeper price point” [70].

Figure 5.4 shows how the different layers of security are implemented in relation to each other. It shows the connection between LoRaWAN’s layer 2 security and the necessary backend security to secure the server side in the network after to gateways.

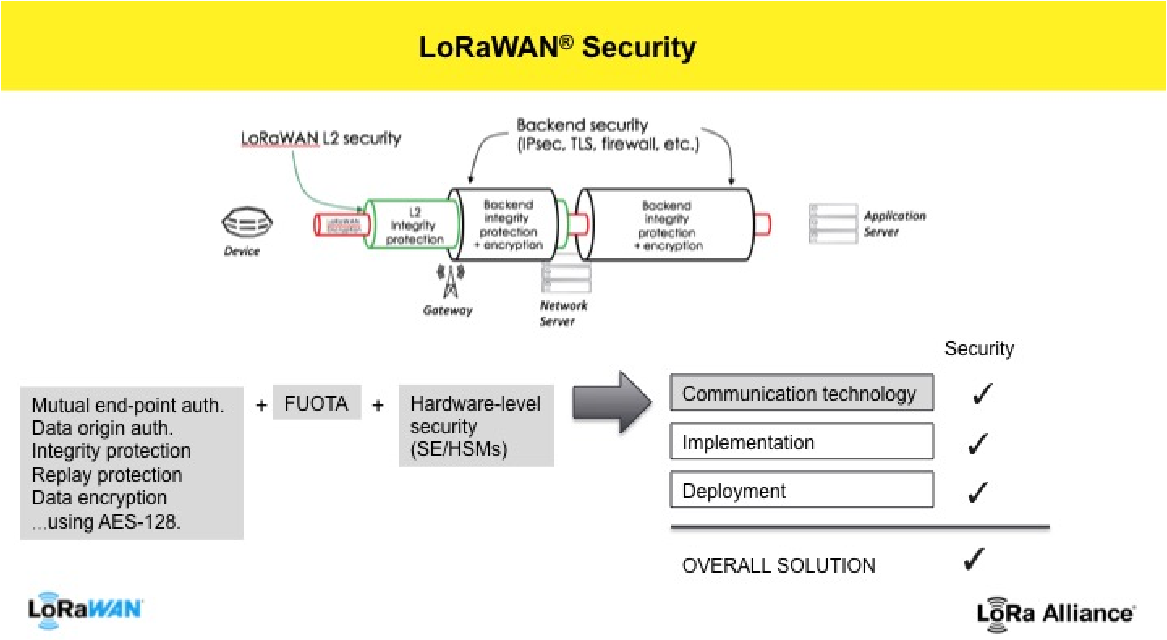

Figure5.4: LoRaWAN security overview

5.5 Conclusion

LoRa and LoRaWAN is a Low Power Wide Area Networking (LPWAN) technology well suited for certain Internet of Tings (IoT) applications. It`s a technology with a low power consumption, low implementation complexity, low cost, and high scalability. The weaknesses of LoRaWAN are poor implementation of QoS, poor latency performance and low bandwidth.

The biggest competitors to LoRaWAN are NB-IoT and LTE-M, they also appear to be the preferred technologies for Norwegian telecom operators due to weaker security in LoRaWAN.

The security in the technology is primarily implemented in LoRaWAN, with limited implementation in the physical layer. The technology has been criticized for being vulnerable to cyber-attacks, although the manufacturers and allies behind it describe the security of the technology as strong.

CHAPTER

SIX

IPV6 SECURITY CHALLENGES

6.1 Introduction

As IPv6 adoption continue to grow, security concerns start to arise. Some problems are inherited from IPv4 and others are new and specific to the new protocol. Over the years security issues have been discussed and mitigations proposed. This paper explains the relevant parts of the IPv6 implementation to form a basis for the reader to understand these security issues. The paper also presents some known security issues and their suggested mitigations.

6.2 IPv6 Implementation

This chapter provides a short overview of the IPv6 implementation and how it differs in some respects from IPv4.

6.2.1 Neighbor discovery

Neighbour discovery (ND) is a protocol used by IPv6 to discover nodes on the same link. It determines link-local addresses and the presence of routers. ND is also used to maintain information about other nodes reachability over time [16]. Some of the problems this protocol solves are Router Discovery, Prefix Discovery, Address Auto-configuration, Neighbour Unreachability Detection, and many more. Router Discovery lets a node know which routers are present on the link. Prefix Discovery tells nodes a set of address prefixes to allow nodes to distinguish between on-link destinations and off-link destinations. Address Autoconfiguration provides a set of mechanisms for a node to configure an address for one of its interfaces in a stateless fashion. Neighbour Unreachability Detection allows a node to detect nodes who are no longer reachable on the link.

6.2.2 Address assignment

There are three main ways a host can get assigned an IPv6 address, Stateless Address Autoconfiguration (SLAAC), DHCPv6 or static assignment. Which assignment method used depends on the setup and what type of node it is, for routers and servers it might make sense to use static assignment, and for mobile devices it might make sese to assign using SLAAC or DHCPv6.

6.2.3 DHCPv6

DHCPv6 functions in a manner very similar to DHCPV4. It can be used both with and without SLAAC and when it is used with it will configure only the network subnet prefixes for the address, and let SLAAC handle the interface identifier. When used without SLAAC it functions the same way as for IPv4, configuring both a prefix and an identifier. Problems can arise however when using DHCPv6 to configure entire addresses ad we will see later when discussing security.

6.2.4 Stateless Address Autoconfiguration (SLAAC)

Stateless Address Auto-configuration (SLAAC) is one of the ways hosts on an IPv6 link can obtain an IPv6 address. It requires no manual configuration from IT-personnel and allows a host to obtain bot link local addresses and global addresses if a router is present [14]. Hosts generate their own addresses based on prefixes (topological) and can use several methods to generate an interface identifier. Link-local addresses use a well-known prefix: FE80::, this allows hosts to configure an address without having to know anything about the link they reside on. This means links do not need a central addressing agent such as a router or DHCPv6 to function properly, and machines on the same link can communicate with one another. Global addresses get their prefix from a router by means of Router Advertisement (RA). A router in the link will periodically advertise itself with information about the subnet prefixes of the link. Hosts will use this information to assign an address for themselves. Often a host will ask the router for the information if it does not receive an RA in time via Router Solicitation (RS).

Getting the prefix for the link-local and global addresses is straight forward but choosing an Interface Identifier (II) is not. First the method of selecting IIs should be determined. Hinden and Deering [5] states that an II should be derived from the interfaces IEEE 802 48-bit MAC address or IEEE EUI-64 identifiers. This worked fine until questions about security were raised. It turns out having predictable addresses can lead to problems when exploited by malicious actors. Today IEEE EUI-64 identifiers should not be used [71], instead random identifiers are preferred. If SLAAC is used in combination with a DHCPv6 server IT-personnel can choose the scheme for IIs. This is not as secure as random IIs even when setup correctly. Often one will see low byte orderings similar to what was usual with IPv4 and even using IPv4 addresses as IIs is common. [71]. This can lead to clustering of addresses in the address space and make the network vulnerable to reconnaissance.

Second, the II needs to be unique within the link, thus a mechanism for addressing collision is needed and is solved using Neighbour Discovery. A host will send out an ND packet with its tentative address and if another host responds, the address is duplicate.

Static address configuration

Static address assignment is mostly used when configuring servers and other static equipment and is done by hand. When assigning addresses this way one will often see problems, again, related to security discussed later. Static address configuration should be avoided in most cases.

6.2.5 Header format

The new header format in IPv6 offers greater routing efficiency and allows for more features than IPv4. The IPv6 header removes several fields found in the IPv4 header and places others in so called extension header [4] These extension headers are placed between the IPv6 header and the upper-layer protocol header. This format allows routers to ignore these extension headers which are only processed at the final destination. In IPv4 if there were any options the router had to go through and process all of them. This makes routing of IPv6 packets more efficient since the router does not process extension headers. The header length field from IPv4 has been removed since IPv6 headers are constant length thanks to any options needed being placed in the extension headers, other fields which have been removed are Identification and flags.

6.2.6 Authentication and privacy capabilities

In IPv4 Authentication and privacy capabilities through Authentication Header (AH) and Encapsulating Security Payload respectively (ESP), were optional to implement but in IPv6 it is a mandatory part of the protocol implemented through extension headers [11]. AH and ESP is part of the IPsec protocol suite which together with Internet Key Exchange (IKE) allows for secure encrypted communication on the IP layer. IPsec is often used to facilitate Virtual Private Networks (VPN) between hosts.

6.3 IPv6 Security Challenges

This chapter presents some IPv6 security challenges and discusses mitigation strategies for these issues.

6.3.1 IPv6 reconnaissance

Often the first step in an attack on a network is the attacker trying to gather information about the network. Interesting information includes the topology of the network, connected, hosts and services that run on these hosts. The topology of a network can be useful for understanding how to move through it and connected hosts can reveal information about themselves which the attacker can use to exploit known vulnerabilities in running services. The more an attacker knows about the network and its hosts, the easier it will be to successfully launch an attack and evade detection [72] This method of probing networks is often referred to as network reconnaissance.

In an IPv4 network, reconnaissance is a trivial matter. The entire IPv4 address space is only 2^{32} addresses which is around 4 billion, and it can be scanned within hours with powerful enough equipment. Most IPv4 subnets are /24 networks which mean that the first 24 bits of the address describes the network while the last 8 are node addresses. This means that a typical IPv4 network only has 256 addresses and can be scanned in seconds using only a laptop. In IPv6 networks the addresses are 128 bits which results in an address space of 2^{128}, this space is so large that it is unfeasible to search through all the addresses. Even when searching through local networks the standard size of subnets are /64. Even though the size of the IPv6 address space large, it does not mean that it is impossible to scan these networks and successfully gather enough information to launch an attack [71].

Based on which method is used to assign addresses in a network, an attacker can use heuristic patterns to find active hosts without scanning the entire address space. Depending on the method for assigning IPv6 addresses in the network, the host density goes up or down. Using SLAAC with semantically opaque IIDs will give lower host density than manually configured addresses, the latter often resulting in low-byte addresses in which most of the bytes of the IID are set to 0 except for the least significant byte. Other examples of IID schemes are IPv4 based addresses, service port addresses and wordy addresses. [71]

6.3.2 Activity correlation and tracking

Misconfigured IPv6 addresses can be used to correlate a user's activity over time, with IEEE-based IIDs the lifetime of the address is the same as the lifetime of the network interface. Often this is the lifetime of the device. Non-changing addresses can therefore be used as identifiers to correlate non related activity [73] across networks. IPv6 addresses as identifiers are a problem, because these addresses are required and cannot be hidden or encrypted easily. Although a host changes its IPv6 address frequently to avoid being identified, other longer-lived identifiers may exist. Thus, IPv6 is only a part of a larger problem related to this type of fingerprinting.

As described in Section 6.2.4 an IPv6 address is made up of two parts, a topological portion and an interface identifier portion. Hosts that receive traffic from a mobile device with an IEEE based IID would be able to passively observe the topological portion change as the mobile device moves between links. This could be used to track the movements of the mobile device. An attacker who learns of the interface address of a mobile device could probe other networks for the presence of the same interface address using ICMPv6 requests. The user of the device could block such requests, but the first-hop router will answer with an error if the address is not present in the link and does not respond at all if it is present. This is a new security issue with IPv6 since IPv4 devices usually get new and totally different addresses when moving between networks.

6.3.3 Rouge Router Advertisements - Spoofing

On IPv6 links routers send router advertisements (RAs). Sometimes due to administrator misconfiguration or malicious actors, false RAs are sent out onto the link. Rogue RAs can cause disruption in the network since hosts use RAs to determine the links default router address and if they are using SLAAC the network prefix part comes from RAs. When there is more than one RA on a link, a host may assume the wrong prefix for SLAAC but get the right default router address. This will cause issues.

There are several ways to mitigate rouge RAs, some of these include RAGuard, SEcure Neighbor Discovery (SEND), and others described in RFC 6104. RAGuard and SEND focus on snooping RAs and dropping those who are not legit. Other approaches rely on the administrators not making errors when configuring RAs, but this cannot be expected to happen. Therefore, protocols such as SEND and RAGuard seem the best candidates to mitigate this issue.

SEND

Originally IPsec was to be used to protect the Neighbour Discovery Protocol (NDP), but due to limitations in IPsecs usability in this circumstance it is not a viable solution. IPsec is limited to manually configured security associations, and the number of associations needed to protect NDP is large. SEND aims to protect NDP without the use of IPsec. [74]

SEND requires the certification of routers before a host can it as a default route, Cryptographically Generated Addresses are used to make sure the sender of an NDP message is the owner of the address and public key cryptography is used to ensure the sharing of such addresses. RSA is used to sign Neighbor and Router discovery, making sure the messages come from legit sources. Hosts uses their private key to sign messages and the receiving hosts check that signature with the senders public key. To protect against reply attacks all messages are timestamped.

SEND however is a rather extensive and complex addition to a network and relies on hosts to implement it's functionality In networks with older hosts or lighweight IOT hosts SEND might not be supported by everything. Therefore it is not applicable in all circumstances. [75]

RA guard

Since the implementation of SEND is not applicable in every network and can be relatively complex, RA guard was developed to be a lightweight solution to spoofing attacks in a network [75] RA guard sits between hosts and routers in the network and monitor RA packets for rouge RAs. Only approved RAs are allowed and non legit RAs are silently dropped. Usually RA examines packets and determines based on sender address wether or not it should be approved.

Since some hosts may not implement SEND, RA guard can be used to supplement a SEND implementation and make sure rouge RAs cannot attack the part of the network which SEND does not cover.

6.4 Summary/Conclusion

IPv6 aims to fix a lot of problems with IPv6 and simplify the IP protocol. In doing so a greater focus on security have been adopted over the years. Some problems such as recognisance are still problems today but mitigation factors have been implemented. Other problems such as being able to track users across networks are new and require new additions to the protocol. This shows us that creating a protocol that is free from security flaws is hard and increases the complexity.

CHAPTER

SEVEN

5G ANALYSIS

7.1 Introduction

In today's society, people rely on Internet access. There are several technologies out there that intertwine and give access. One such technology is Wi-Fi, which makes it possible to connect to the Internet wirelessly.

Another technology that gives Internet access wirelessly is 4G. 4G is the fourth-generation mobile broadband technology and is universally used by mobile devices.

In 2021, there has been deployment of a new technology called 5G. This technology is, as the name suggests, the fifth-generation mobile broadband technology. Whenever new technology arrives, questions should start to arise, such as: how secure is this technology? In this paper, introduction to 5G technologies and analysis of 5G and its risk is performed.

Before jumping into any risk analysis (RA), we need to have some basic understanding of 5G and radio access networks (RAN). In this chapter, 5G standards and usage of 5G are elaborated on. The next chapter, Technologies, is also introductory, but it is separated from this chapter because of its size.

7.1.1 Overview of 5G

5G is a technology currently being deployed around the world [76]. As an example, Telenor, a Mobile Network Operator (MNO) in Norway, have deployed 5G in several counties and are planning to further expand the 5G network in 2022 [77]. By deploying 5G, MNOs provide high speeds to the end-user, decreased latency, increased network capacity, and increased availability.

These factors in turn empower communication that can be used for many use cases. In the health industry, for example, 5G might be used to perform remote surgery. By interconnecting IoT devices, medical procedures could be simplified, tasks could be completed quicker, and patients could get more quality help.

Another use case for 5G is Vehicle-to-everything (V2X) which connects the vehicle to other entities. The vehicle might connect to other cars, traffic lights or satellites. All this to reduce traffic jams and traffic accidents.

Because of these use cases (and more), 5G is expected to be utilized to a high degree in the next years [78].

7.1.2 Standards in 5G

The International Telecommunications Union Radio sector (ITU-R) created IMT-2020, which is a set of requirements for 5G. It is considered to be the 3rd Generation Partnership Project (3GPP) that will specify 5G by fulfilling these requirements. The reason for 3GPP being mainly considered for this is because of their success with LTE [79].

3GPP is of course not the only organization which creates and specifies 5G technologies. As an example, LoRa could be considered a competition to 3GPP NB-IoT. There are also organizations that try to direct the 3GPP 5G standard more into a particular field of interest (e.g., 5GAA).

By having 3GPP create a central standard for 5G, it would make compatibility between 5G and other technologies easier. If there are several different 5G standards in high usage it would create unnecessary complexity. It does also have its drawbacks to have a single shared standard, as entities from left and right want an input into how the standard should become.

In this paper, the focus will be on the 3GPP 5G standard.

7.1.3 The use of 5G

As reported by ITU-R, mobile video traffic, machine-to-machine (M2M) traffic, and general traffic will increase exponentially towards the year 2030 [80]. This means that the need for bandwidth will increase. 5G is therefore supposed to help fill this demand with the use of mmWave.

An everyday use case that requires a lot of bandwidth is watching high quality videos. As time goes on, video quality might increase, which supports the need for 5G even more.

5G tries to deal with future use cases that do not necessarily exist today as well as the use cases that already exist. For example, IoT is a market that might be used in industry. This is called Industrial IoT (IIoT). IIoT refers to sensors, Cyber Physical Layer (CPS), and machines connecting and talking to each other. Another example of a future use case is that houses will become smarter by interconnecting technology in kitchen equipment, doors, garage, and more. All of these and more use cases contribute to the expected increase in bandwidth.

One of the main reasons for the use of 5G is also its spectrum. ITU-R decided on the spectrums for 5Gs mmWave as shown below [81].

- 24.25–27.5 GHz – global identification
- 37–43.5 GHz – global identification
- 45.5–47 GHz – regional/country-specific identification
- 47.2–48.2 GHz – regional/country-specific identification
- 66–71 GHz – global identification

With the use of the mmWave spectrum, the increasing bandwidth will be easier to handle.

Another 5G advantage is that its technology will be more energy-saving. The Xn interface, for example, will support turning off and on cells to save energy. Energy saving is important not just for businesses, but also for the people. Energy saving will make electricity cheaper and help battle the climate crisis [82].

7.2 Technologies

By having explained some of the use-cases and standards surrounding 5G, a dive into the technology behind it is needed.

Since 5G follows the earlier generations 3GPP systems, the 5G system (5GS) includes components which also is part of 4G. Some of these components are Quality of Service (QoS), lawful interception, and mutual authentication between user and the network. However, 5G is a new generation of telecommunication, which implies new or evolved components.

One of such components that 5G evolved from is 4Gs Evolved Packet Core (EPC). “Evolved Packet Core (EPC) is a framework for providing converged voice and data on a 4G Long-Term Evolution (LTE) network” [83]. Instead of switching voice-packets by circuit-switching and data-packets with packet-switching, EPC puts both data and voice packets on an IP service architecture. 5G evolved this even further by splitting into several Service based-architectures (SBA). This splitting makes for easier programmability which is wanted for MNOs [84].

7.2.1 Network slicing

Network slicing is, as the name suggests, a way of slicing the network. Slicing the network has its purpose when different configurations are wanted for different users. Examples of network slicing is configuration for IoT (low bandwidth), slice for emergency calls, and slice for an industry (military etc).

Network slicing is not something new in 3GPP technology, but there are shortcomings that 5G wants to address. Firstly, UE can only be connected to one Dedicated Core Network (DCN). Secondly, sometimes RAN can’t differentiate which DCN the UE should be in. 5G will try to fix these problems.

7.2.2 CUPS

Another part that has evolved is Control- and user-plane separation (CUPS). CUPS talks about the separation between the control plane and the user plane. The control plane is about controls such as QoS and user authentication, while the user plane is about sending data. By separating the control plane from the user plane both can separately scale as they wish.

EPS had its problems scaling the user plane. 5G tries to solve this by having a modern design which considers the user plane from start to end.

7.2.3 Private Networks

5G has also been designed to provide private networks. As an example, a factory might decide to deploy 5G to help automate processes. A private network deployed in a factory could either be a Stand-alone Private Network (SNPN) or Public-network-integrated non-public network (PNI-NPN). SNPN is when both the core network and RAN are deployed in the factory itself. PNI-NPN is when the core network is shared between the PLNM and NPN.

7.2.4 NG-RAN

NG-RAN is the radio access network for 5G. NG-RAN is either a gNB node or a ng-eNB node. The gNB node uses NR, while the ng-eNB node uses LTE. This is a new concept, as former generations have been using one type of radio access technology (RAT). Since 5G will be using both NR and LTE, the system is more complex.

The nodes support two interfaces, Xn and NG. The Xn interface goes in-between the nodes, while the NG interface goes between the 5GC and NG-RAN. These interfaces use the IP/SCTP or IP/UDP stack (depends on if it is control plane or user plane).

7.3 Case description

The previous two chapters, introduction and technologies, should have given some idea of how the 5G system (5GS) functions. Before the RA is performed it is essential to know what is to be analyzed and what is not to be analyzed, what unacceptable risks are and so forth. All of this is following the ISO 27005 standard. In this chapter the prerequisite for the RA is presented.

7.3.1 Purpose

The purpose of this RA is to illuminate the risks surrounding the 5GS. From this RA the hope is to inspire others to do a more in-depth RA with this paper as an overview.

7.3.2 Scope

The scope of the RA is the 5GS and its related parties. However, it will not be an in-depth RA, as that would indefinitely cause scope creep. The reason for this scope is because of lack of sufficient knowledge of any sub-area of the 5GS. This RA should therefore not be regarded as a complete RA of the 5GS. The scope is a broad overview of the concepts in 5GS. As such the RA will not include all assets of the 5GS, threats regarding those assets, vulnerabilities, and not all risks present in the 5GS.

7.3.3 Assumptions and Constraints

The reader of this paper should have knowledge of the 5GS. The reader should also understand the ISO 27005 standard. The RA is constrained by a limited time of 90-110 hours of work.

It is assumed that foreseen use cases, such as private networks and IoT, are real. It is also assumed that the stakeholders in this RA have "moderate" security measures in place. This is explained more in detail in the identification phase of the RA.

7.4 Methodology

Previous chapters have explained the purpose of this paper, the technology behind the 5GS, the scope of the RA and the assumptions and constraints. Next is to present the method used for this RA and definitions needed for the RA.

7.4.1 Methods

The RA will follow the ISO 27005 risk assessment method. At the same time, the book "Management of Information Security Sixth Ed" Chapter 6 is used as inspiration on how to perform this RA.

7.4.2 Stakeholders

Events can be defined as something happening to a stakeholder that negatively impacts day to day business. Regarding the 5GS, the stakeholders are:

- MNOs
- Telecom equipment manufacturers
- Cloud infrastructure providers
- Producers of net-connected devices (mobiles, computers, cars).
- Everyday people

7.4.3 Intervals

Here we define intervals on likelihood and consequence. In the table below the likelihood scores are defined. This interval does not stand for the full view of all stakeholders because of their diverse needs. A table for each stakeholder could have been presented, but because of constraints as explained in "Case description" this is not feasible. It should also be mentioned that this table does not describe the frequency of an event happening to (for example) all MNOs combined, but rather for each MNO individually. If a risk is "Almost certain" then every MNO would have the event happen several times a year.

Table7.1: Likelihood scores

Likelihood score	Description	Frequency/Percent
5 - Almost certain	100% likely in the next 12 months	May happen several times a year
4 – Likely	75% likely in the next 12 months	May happen once every year
3 - Probable	50% likely in the next 12 months	May happen once every 5 years
2 - Unlikely	25% likely in the next 12 months	May happen once every 10 years
1 – Rare	5% likely in the next 12 months	May happen once every 20 years
0 – Won't happen	0% likely in the next 12 months	Will never happen

Below is a risk impact table. The same is true here as for the likelihood table (different for each stakeholder).

Table7.2: Risk impact table

Rank	Example	Productivity hours lost	Financial impact
5 - Severe	Multi-day interruption, major exposure of data	24	1 000 000 kr
4 - Major	One day interruption, exposure of data	8	100 000 kr
3 – Moderate	Multi-hour interruption, minor exposed data	4	1000 kr
2 - Minor	Multi-minute interruption, no exposed data	2	200 kr
1 - Insignificant	No interruption, no exposed data	0	0
0 – Not applicable	No impact	N/A	N/A

Below is the information classification table on the CIA triad. This is used for giving a sense of how precious an asset is, or how dangerous a risk is.

Table7.3: Information classification table

Rank	Confidentiality	Integrity	Availability
1	Open	No influence	No influence
2	Internally	Expected integrity	2 days
3	Confidential	Depends on situation	4 hours
4	Highly confidential	Critical	Immediately

7.4.4 Risk acceptance

Risk acceptance is typically formed between the ones doing the risk assessment and the stakeholders. However, as there is no definite contact for establishing correct risk acceptance the accepted range is just set to be:

- Likelihood “unlikely” or less
- Impact “minor” or less

This is done as to keep this simpler and not create additional speculative accepted scenarios.

7.5 Risk identification

In the earlier two chapters “Case description” and “Methodology” the basis for the risk analysis was formed. With a context established for the 5GS, and with a method to analyze the 5GS, it is time to determine risks. Before any risk can be defined the assets, threat agents, threats, security controls and vulnerabilities must be presented. For each of these, three things identified will be pointed out as being the most important ones. In this chapter all of these will be identified as to help find risks.

7.5.1 Assets

Starting with the identification phase, the assets are presented. Table 7.4 shows information assets for the primary stakeholders. In the columns on the right the confidentiality, integrity and accessibility score are presented based on the information classification Table 7.3. The score column is the total importance of the asset for the stakeholder. It is calculated by taking the highest value from the CIA triad. Of course, this is not the whole picture for an asset, as its importance also comes from generation of revenue, profitability, expensiveness, cost of securing and so on. But this is sufficient to give an indication of its importance.

Table7.4: Information assets

Asset	Description	Stakeholder	C	I	A	Score
LTE	4G Air Interface	MNO	1	4	4	4
NR	5G Air Interface	MNO	1	4	4	4
5GC	5G Core network	MNO	4	4	4	4
5GS	The whole 5G System	MNO	4	4	4	4
IoT	IoT device in factory or similar	MNO, Industry	3	4	4	4
NG-RAN	NextGen Radio Area Network (NG-RAN)	MNO	3	4	4	4
Network equipment	Switches, routers etc.	MNO	3	4	4	4
Filtering	Firewalls, IPS etc.	MNO, Industry	4	4	4	4
UE	User Equipment is scarce for end-users	Everyday people	3	3	3	3
UE data	Data stored and data transmission between UE and services	Users	3	3	3	3
5G area	An area that has 5G available	MNOs, everyday people	4	4	4	4
Cloud infrastructure	Cloud storage	Everyone	4	4	4	4
Internal documents	Documents confidential to the organization	MNOs, Industry	4	4	3	4
End-user	The user of the 5GS (calls, internet etc.)	MNOs	4	4	4	4
Car	Car connected to the 5G network.	End-Users	4	4	4	4

The three most important assets are 5GC, LTE and NR. The 5GC is as stated, the core of the 5GS. It is therefore sorely important. LTE and NR are both extremely important because without it 5G would not be able to perform its primary goal; to provide Internet access wirelessly.

7.5.2 Threat agents

Next, the threat agents in are presented. Threat agents against the 5GS ranges from non-adversaries to Advanced Persistent Threats (APTs). The list is prioritized from the highest capable threat agent to the least capable.

Table7.5: Threat agents

Threat agent	Description
APT	Advanced persistent threat. Example: fancy bear, Lazarus Group, equation group. Motivated by political agendas and on a few occasions financial gain.
Organized group	Motivated by financial gain. Typical ransomware groups such as REvil.
Hacktivist group	Motivated by political agendas. Example: anonymous
Individual hacker	Motivated by political agendas, “trolling” or financial gain. Moderate to high skill in hacking.
Script kiddie	Typically inspired by movies and want to gain reputation or just be able to hack something. Very low-level skills.
Insider	Someone on the inside exposing assets. Motivation includes blackmail, financial gain, or revenge.
Non-adversary	Accidental takedowns of system or accidental exposure of assets. Motivation is non-related to the event.

7.5.3 Threats

Below are categories of threats to the 5GS. There are three columns that gives a form of prioritization for each category of threat. The columns probability of occurrence, success and cost of securing are based on subjective assessments.

Table7.6: Threat categories

Threats	Description	Probability of Occurrence	Probability of success
Information Extortion	Blackmail on personnel	Rare	50%
Software attack	3GPP 5G will utilize software more than before. An attack could happen.	Unlikely	90%
Espionage	Spying on industries etc.	Probable	50%
Nature	Earthquakes, fires etc.	Rare	5%
Social Engineering	Tricks personnel into giving information or access.	Almost certain	5%
Human error	Accidental error made by individual influences business.	Almost certain	5%
Denial-of-Service	Denial of service on the 5GS.	Almost certain	1%
Theft	Stealing assets from the 5GS.	Almost certain	90%
Unauthorized access to 5GS network.	Access to a MNOs 5GS.	Probable	5%
Revenue loss	Loss of revenue is for industries extremely damaging	Almost certain	•
Sabotage or vandalism	Destroying assets directly or indirectly.	Likely	95%

The three biggest threats in this list are social engineering, Denial-of-Service, and revenue loss. Social engineering is dangerous because of its effectiveness. You do not need to be a techie to understand that people are by far the weakest link. Denial of service is dangerous because it's easy to perform and extremely damaging for day-to-day business. A successful Denial of service attack can render businesses useless for days. Revenue loss is dangerous because of its importance to get things done. Without money the train stops running.

7.5.4 Controls

Basic control domains in the 5G standard will be listed below. In addition, a few specific controls are also listed. To see even more detailed security controls, present in the 5G standard, see 3GPP TS 33.501. Specific controls for the stakeholders are be excluded as they would be too speculative.

Table7.7: Controls

Control	Description	Control effectiveness	Protected assets
4G security	5G will include already existing security features present in 4G [85]	This effectiveness is high, as 4G security is not something easily bypassed by normal individuals.	All
5G trust model	The further away the technology is from the core network, the less it is trusted.	This is set to be medium to high because it is a great concept, however it could be faulty. 5G is still new, so time will tell if it is medium or high.	All
Network access security	“Set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN to AN for the access security.” [86]	This is high effectiveness as it protects the system from unauthorized access.	LTE, NR, End-user, UE data
Network domain access	“The set of security features that enable network nodes to securely exchange signaling data and user plane data.” [86]	Effectiveness is high because of its prevention of eavesdropping and hijacking of data transfers.	5GC, 5GS
User domain security	“The set of security features that secure the user access to mobile equipment.” [86]	This is medium, as it protects user equipment. However, it is not critical for the 5GS to operate.	End-user, UE-data
Application domain security	“The set of security features that enable applications in the user domain and in the provider domain to exchange messages securely.” [86]	Effectiveness is high because without it eavesdropping, replay attacks etc. would maybe be easily performable.	End-user, UE-data, Cloud infrastructure
SBA domain security	“The set of security features that enables network functions of the SBA architecture 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.” [86]	High effectiveness because of its variety of security functions.	5GS
Visibility	“The set of features that enable the user to be informed whether a security feature is in operation or	Medium effectiveness as this does not protect	End-user,

The three most important controls in place in the 5GS is; Network access security, as it protects the two of the three most important assets; SBA domain security, as it protects a by numerous security functionalities; and Network domain access, as it protects one of the three main assets.

7.5.5 Vulnerabilities

Threat agents needs to use vulnerabilities in the 5GS to be able to obtain their goal. Below is a table of possible vulnerabilities in a 5GS.

Table7.8: Vulnerabilities

Vulnerability	Description	Assets
Insufficient risk management (RM) program	Risk management is needed to keep risk at a minimum.	All
Absence of compliance with 3GPP standard	3GPP standard is regarded as the main standard of 5G.	UE, NR, LTE, IoT, 5GC
Inadequate physical security	Bad physical security for equipment or people.	LTE, NR, IoT, End-Users
Poor management processes	Lack of change management, configuration management etc.	5GC, IoT, UE-data
Insufficient training of personnel	Personnel needs security awareness	All
Insufficient handling of change in society norms	E.g., corona forced people to stay home.	Cloud infrastructure, Network equipment, Filtering
Lack of physical security	Physical security does not reflect assets importance	LTE, NR, Internal documents, IoT, Network equipment
No ISSP (Information Systems Security Policy) for remote access	When accessing internal assets (e.g., components of 5GS) ISSP is needed	Internal documents, 5GS, 5GC
Bad design of 5GS	A bad design makes the attack surface much more vulnerable	All
Hardware bug	Hardware bug gives some form of vulnerability.	Network equipment, 5GS, 5GC
Lack of diversity	Using the same technology everywhere	All
Misconfiguration of equipment	Equipment is configured in such a way that an adversary can gain access to assets	All
Lack of access control	Access control to internal systems.	All
Jamming/spoofing signals	Jamming or spoofing signals by outputting stronger or an inversed signal which renders communication useless.	Car, End-user, UE-data.

The three most important vulnerabilities to take note of are bad design of 5GS, misconfiguration of equipment and lack of physical security. Bad design will endanger all assets and will be extremely difficult and time consuming to try to fix. Misconfiguration of equipment is dangerous because of the single fact that if just one out of a thousand pieces of equipment is wrongfully configured, the adversaries will get a good chance of getting access to valuable assets. Bad physical security is more dangerous now because 5G mmWave requires UE equipment to be close by. This means equipment might be more accessible for adversaries.

7.5.6 Risks

Assets, threat agents, threats and vulnerabilities are now identified. Using the identified entities risks can be formed. The threat agents in the risks are the ones seemingly most relevant to the risk. This means other threat agents might also present such a risk.

1. APT exploits bad design and gets unauthorized access to the 5GC. The APT now has access to all assets related to MNOs and partly other stakeholders.
2. APT exploits hardware bugs and spies on industries and/or countries.
3. Individual hacker exploit misconfiguration of equipment and performs theft of UE data.
4. Insider exploits know existence of ISSP and brings confidential documents home, which gets found by adversary. From this point, an adversary could use a chain of vulnerabilities to get to its primary objective.
5. Organized group exploits lack of diversity in software (e.g., Software defined network) in the 5GS and gets full access to every unit using that software.
6. Organized group exploits insufficient training of personnel and uses social engineering to get access to cloud infrastructure.
7. An absence of compliance with the 3GPP standard makes it hard to comply with other technologies which causes loss of revenue.
8. Script kiddie exploits insufficient RM program (this can cause a range of other vulnerabilities) and get unauthorized access to the 5GC.
9. Script kiddies exploits poor physical security and causes denial-of-service by destroying network equipment.
10. Organized group exploits poor configuration management and finds a single node exploitable to a software attack. The adversaries get access to every asset related to the MNO.
11. A third-party contractor (insider) has access to the 5GS as to do administrative tasks, but because of lack of access control decides (and is able) to steal information/perform espionage.
12. Organized group utilizes poor RM and gains access to the network slice for emergency calls, which disrupts the service and causes life threatening situations.
13. APT takes over IoT devices in critical infrastructure (power grid etc.) by exploiting bad physical security and disrupts the infrastructure.
14. Individual hacker spoofs or jams signal to car (V2X), which causes crash and might cause revenue loss for MNO and End-user.

7.6 Risk analysis

In the identification phase the assets, threats, threat agents, vulnerabilities and risks were listed. With these listings it is still unknown what the severity of the risks are. Some risks might be present but inside accepting range, while some might be outside the accepted range and need to be dealt with. To decide which risks are acceptable or not, the risks will be defined with two characteristics: likelihood and impact. These two characteristics are defined in the Method chapter.

The characteristics for each risk will be put to light in a risk matrix. Risks that are outrange of accepted range can then be handled. The placement of the risks is based upon the opinion of the writer of this RA. In the table below, the risk matrix is presented.

Severe	R5, R7, R12	R1, R2, R3, R6, R13	R10	🟥	🟪
Major	🟩	🟨	R9, R11	R14	🟥
Moderate	🟩	🟩	🟨	🟨	🟥
Minor	R8	🟩	🟩	R4	🟨
Insignificant	🟩	🟩	🟩	🟩	🟩
	Rare	Unlikely	Probable	Likely	Almost certain

From this matrix five risks will be taken into the risk treatment phase. These are picked out based upon the placement in the matrix. The five most important risks are R4, R9, R10, R11, R14. These risks will be the ones taken into the risk treatment phase. These risks were taken out because of their position in the matrix and because of the assets they endanger.

7.7 Risk Treatment

Till now, the risks have been listed and set into perspective from the risk acceptance criteria. To reduce risk, controls will be modified, introduced, or removed.

7.7.1 Treatment overview

Here is an overview of the treatments that should be put in place.

- T1: Have ISSP in place.
- T2: Improve the physical security of equipment.
- T3: Establish configuration management.
- T4: Have policy on access procedures.
- T5: Automatic spoofing or jamming detection.

7.7.2 Treatments

Here are details surrounding the controls. A description of the control is given, the estimated remaining risk after implementation is stated, the current risk, time for implementing the control, cost for buying items, cost for operating controls, time needed for maintaining control at sufficient levels.

Table7.9: Treatments

Treatment	Risk	Description of control	Residual risk	Current risk	Time for implementing	Cost	Operation costs	Time for maintainace
T1	R4	Have an ISSP in place and make sure that employees have read and understood the policies.	2x2	4x2	~24 hours	0,- kr	0,- kr	~7 hours each year
T2	R9	Whitelist access to equipment by locking equipment up behind walls or other physical objects.	2x4	3x4	~1 hours pr. equipment	1000,- kr pr. equipment	~500,- kr yearly per equipment	~10 minutes each year pr. equipment
T3	R10	Have proper configuration management.	2x3	5x3	~24 hours	10 000,- kr	10 000,- kr for any software helping the process.	~7 hours each 6 months
T4	R11	Have strict and clear procedures written down into policies on how access to the 5GS is supposed to happen.	2x4	3x4	~72 hours	0,- kr	0,- kr	~7 hours each year
T5	R14	Automatic detection of spoofing or jamming by protocol or other technologies.	2x4	4x4	~100 hours	10 000,- kr for each car	0,- kr	~7 hours each year

T1 has a lowered residual risk because of the way the ISSP should be written. The company would distance itself from the action, whilst also increasing awareness for the employees that this is not accepted. For T2 there is a lot of work to do to protect the assets, but in turn the consumers will be more satisfied with the service. This does not do much for consequences, but it does lower the frequency of occurrence.

T3 is important, as if even one out of a thousand nodes are not up to date, the adversary could gain access. Configuration management tries to nullify this by either software and/or a strict process in deploying equipment. This does necessarily lower the consequences, but it does lower the probability of occurrence. T4 is mainly about creating awareness and creating a controlled environment where least privilege is important. It does decrease frequency, but not as much the consequence.

The last treatment, T5, decreases the frequency, but it is unknown of how much. To make an estimate here would need further research into technologies and standards. This is therefore an experience-based estimate. There exist technologies that already do prevent spoofing and jamming, but since 5G is a new technology, new techniques might occur, and therefore this needs to be considered once again.

7.8 Conclusion

7.8.1 Further work

Further work would be to go more in-depth into specific areas of the 5GS. LTE is already tested by time. NR, however, is not. NR could therefore be a suitable place to perform an RA. Preferably the RA should be performed by competent people who are familiar with the 3GPP 5G standard and NR.

7.8.2 Conclusion

5G is a complex system that will probably be highly utilized in the coming future. With the 3GPP standard being set into stone, only time will show how secure or insecure the 5GS is. Stakeholders surrounding the 5GS should be aware of their most valuable assets. This includes assets such as LTE, NR, and the 5GC. At the same time, they should be aware of threat agents and threats by performing threat hunting. Stakeholders should manage the existing controls in the organization and understand what threats it mitigates and what assets in the 5GS it protects. From risks such as V2X jamming, lack of policies, improper configuration management, and poor physical security could be identified and reduce uncertainty of an organizations risks.

CHAPTER

EIGHT

PROPOSE SECURITY SOLUTIONS FOR IT AND FOR REAL TIME APPLICATION FOR 5G

Abstract

5G is quickly emerging to become the next standard in mobile data networks. It brings with it updated capabilities compared to previous technologies. It may also bring with it new issues in security, privacy and in general concerning confidentiality, integrity, and availability (CIA). This paper investigates some of the implications of securing real-time application of 5G. Other potential issues in the 5G environment are also investigated and a first look at these paired with relevant academic literature serves to provide examples on how to thwart, mitigate or relieve such issues.

8.1 Introduction

With the imminent deployment of the latest 5G technology, new issues may arise in terms of security. What security concerns do we face when transitioning to a new cellular network technology? Does it address the security issues from previous generations? Implementing a new technology presents the industry with an opportunity to change the direction they are heading in and to improve on past issues. If security was not at the forefront previously, there should be ample opportunity to include it as such this time around.

5G will succeed the current iteration that is the 4G Long Term Evolution (4G LTE) mobile network. One is already aware about a plethora of security issues in connection with the current mobile network. An example of this are the receivers or eNodeBs at base stations that receives the incoming connection from mobile devices. These receivers may be at the mercy of hardware, firmware and/or software that works together to keep the service running. If this eco-system is not properly configured and regularly updated, the eNodeBs may be susceptible to vulnerabilities and other threats. In the LTE network environment, User Equipment (UE) may be compromised by malware and/or malicious code in such a way that the equipment is rendered unable to connect to the 4G LTE and the user is denied normal network service. Another malware attack may involve multiple instances of UE that together forms a botnet that may disrupt normal service of the radio network provided by a mobile carrier. A mobile carriers' own network component may also be infected with malware, possibly granting the malware the ability to modify configurations of gateways and log network activity. The 4G LTE network is also susceptible to unlicensed rogue base stations that are imitating legitimate base stations provided by legitimate mobile carriers. These base stations take advantage of the tendency in phones to connect to the base station that is the closest to it and/or with the strongest signal. In addition, phones are compatible with legacy technology to ensure that network service is available even when in remote areas or areas where newer technology is unavailable. An example of this legacy technology is 2G GSM. With modern hardware and software, one can recreate the 2G GSM functionality in these rogue base stations. There are possible privacy concerns regarding these base stations and whether the malicious actor operating the station can intercept traffic and determine the whereabouts of users. Another aspect is the criticality in emergency situations where phones need to be able to alert emergency health services to an event, such as if someone were to have a heart attack. If the base station is unable to forward this information because of it being illegitimate, lives may be lost [87].

8.2 Securing the transition to 5G

The transition to a full 5G network will take some time. Therefore, the transition is envisioned to take place through interim periods that utilize the capabilities of both older components and new components. [88] points to different configurations of the 5G specification through which 5G can be deployed. Two configurations are the 5G standalone (SA) and the 5G non-standalone (NSA) scenarios. The 5G NSA may in many cases initially be at the forefront of the transition for many service providers, due to it leveraging the existing 4G LTE Evolved Packet Core (EPC) present in the existing infrastructure of many providers. The 4G LTE EPC works together with the 5G NSA to take advantage of the new 5G new radio (NR). The 5G SA on the other hand, will implement the full range of security features as specified by the 3rd Generation Partnership Project (3GPP) in an all-new 5G core network.

Wazid et al [89] outlines some of the possible attacks that can take place in a 5G-enabled IoT environment. Eavesdropping can be executed on communication channels to intercept or discover information communicated between two parties or entities. It may provide an attacker with the means to launch new attacks. Traffic analysis is a passive type of attack that monitors the encrypted flow of information to assess and analyze what the contents of it might be, what the identities of the parties involved are, and where the information may originate from [90]. When network resources are requested in such a way that the resources are stretched thin, resulting in end-users being denied normal services from the network, one is dealing with a Denial-of-Service (DoS) attack. The servers are rendered unable to process incoming requests from end-users. These types of DoS attacks are often carried out through means such as the UDP network packets in which ports on the servers are overrun with packets or abusing the HTTP protocol which requests resources on a server. A DoS attack can also be expanded to a distributed DoS attack by launching an attack from several systems or clusters at the same time against the target. Another way to launch attacks in the 5G-driven environment is database attacks, using structured query language (SQL) attacks, cross-site scripting, or cross-site request forgery attacks. The database attack may target user credentials for example. Lastly, a malware attack may be launched. This attack often assumes the form of viruses, trojans worms or malicious scripts. They can make devices a part of botnets and monitor keystroke activity or spy on the activities performed on the device. The resources, storage capabilities and computing power of the device can be abused. The attacker may also be able to remotely take control of the device and make use of its features remotely. The researchers also note some important security and privacy issues [89]. They point at a lack of robust security schemes which implies that there is a threat of information being leaked, and that data from IoT devices could be disclosed. Another aspect is the transparency or openness in the 5G-communications. The cooperation between such open networks may contribute to attackers being able to launch attacks into other parts of the network. Finally, issues regarding the privacy of sensitive data are noted. Due to the composition of different devices, they run with and on top of different types of hardware and software. The different combinations and agreements on mixing software and hardware may lead to devices being more susceptible to different attacks, such as replay, traffic analysis, man-in-the-middle, and masquerade attacks among others. Owing to these acts of potential manipulation and unauthorized access, user information such as credit card details, date of birth and addresses are at risk of being disclosed. Thus, communication channels in the 5G-enabled communications must be protected against possible attacks.

8.3 Secure real-time application for 5G

Afaq et al [91] notes how the 5G network will bring with it a higher spectrum utilization, higher data rates and increased bandwidth compared to its predecessors. Due to the overall increase in capabilities, the researchers argues that 5G should be able to implement and make use of machine learning (ML) to a larger extent than what may previously have been possible. The network should be smart enough and provide the capacity to utilize ML in real-time to make it more resilient when facing new threats and attacks with evolving characteristics. ML will assist the network with detecting issues on the network, and to hopefully provide solutions in real-time to alleviate the issues. At this point in time ML will assist the IT department and 5G professionals with monitoring and addressing abnormalities and anomalies. In time, one is optimistic about ML assuming an even larger role in the 5G environment and potential successors to 5G where it acts in a more autonomous fashion, maybe even to the extent where it can make its own judgements without assistance or interference from human expertise. At the 5G Core layer, classification ML algorithms and clustering ML algorithms can be utilized to detect anomalies in network throughput and logs and grouping different threats and loopholes in the security of the network. At the access layer or the NR of the 5G environment, ML can be used to pave the way for cooperative knowledge sharing and preservation of privacy between the UE and the NR.

ML has been adopted in finance, healthcare, transportation, and e-commerce to name a few. This increased use of ML means it is important to address the security and privacy concerns surrounding ML techniques. Typically, the traditional approach in ML applications has been that the collected data from systems are aggregated on a centralized server or in a cloud solution to train the ML model [92].

8.3.1 Federated Learning

When looking at ML in relation to the 5G NR and UEs, however, the traditional approach may present an infeasible option on how to implement ML in the access layer. Chen et al [93] points out how it is necessary for the UE to transmit their data to the centralized ML controller to train the model if the traditional approach is used. This can bring with it privacy issues, and be subjected to large constraints on computing power, bandwidth capability and fatigue of available resources in general when one keeps in mind the sheer number of devices connected and the amount of communication performed. In IoT and the 5G network, many connected UEs are present and connected, delivering vast amounts of data over limited wireless resources. To make it both easier for the edge devices or UE to contribute to training a shared and distributed ML model with less amounts of data exchange and to mitigate privacy issues, Chen et al [93] proposes federated learning (FL) to be used. This involves the UE keeping collected or aggregated data to themselves which can reduce the load or congestion on the 5G network and contribute to increased privacy. The researchers speak of both Original Federated Learning (OFL) and their new contribution to the topic which was coined Collaborative Federated Learning (CFL). OFL is characterized by the UEs keeping local FL models to themselves, exchanging these routinely with the base station which aggregates the incoming local FL models from multiple UEs and combines all these datasets to train a global FL model which in turn is redistributed back to all UEs. The advantage of this approach in addition to the privacy aspect is a reduced overhead in data collection when compared to what the researchers call centralized learning (CL) or centralized ML. CFL have a lot of similarities with OFL, but what makes it stand out is its ability to let UEs not only exchange the parameters of their local FL models with the base station, but also with other neighboring UEs. The advantage of this approach is its ability to provide more data samples for training when compared to OFL. Both OFL and CFL and their model training process are more susceptible to imperfect wireless transmission when compared to CL. UEs in CFL also exchanges local FL model parameters with other devices that takes part in the CFL, so that it cannot be stated that CFL is one hundred percent privacy preserving. But OFL and CLF nonetheless provide a better alternative over CL when it comes to secure privacy [93].

Sagduyu et al [94] shows that adversaries can abuse machine learning to launch an attack on spectrum sharing of 5G, and attacks on network slicing. Owing to the distributed and open nature of the wireless domain, jammers and eavesdroppers are susceptible to manipulate the exercising of ML models wirelessly. The first attack jams communication signals and potentially reduces throughput in the network by building a deep neural network surrogate model from the data collected from monitoring the dynamics of the spectrum utilization in channel access and predicting a successful 5G transmission which then fools the 5G base station into making wrong decisions. The other attack is to transfer spoofing signals that replicates the behavior or signatures of the signals that are usually transmitted from a legitimate 5G UE when requesting a network slice. To accomplish this, a generative adversarial network (GAN) is used to create wireless synthetic signals that replicates the behavior of the signals coming from the legitimate 5G UE and which the 5G base station is expecting. If this is accomplished, an adversary may be successful in breaking into the physical authentication layer of the 5G network. The researchers posit a defensive technique to mitigate these attacks by implementing selective errors on the part of the 5G base station that serves to disrupt and the ability for an adversary to train an inaccurate GAN due to the input errors it is receiving from the 5G base station. The same logic can be utilized to confuse the adversary on the spectrum dynamics it is observing, and the subsequent incorrect construction of the surrogate model used [94].

8.3.2 Friendly jamming

Li et al [95] notes that cryptographic techniques are traditionally the most widely used alternative when attempting to safeguard the security of wireless communications. These can be resource-intensive and infeasible to use based on the previous observations on limited resources, bandwidth capacity and an extensive number of connected UEs. It may also be difficult to distribute and manage the keys generated in cryptography in an efficient manner, especially pertaining to the promises of the new 5G technology on ultra-reliable and low latency communications (URLLC). This is a new service category in 5G which aims to improve on reliability from the previous 4G technology and reduce latency, something which is particularly important for example in the rise of autonomous driving or self-driving cars which are sensitive to latency and stable delivery of packets over the network [96]. To safeguard URRLC in the 5G NR, Li et al [95] proposes a friendly-jamming (FJ) scheme to defend against eavesdropping or monitoring on wireless signals. This can be achieved in one way by generating artificial signals that acts as noise transmitted together with the original or legitimate signals from the transmitter or receiver. Another way to achieve it is by deploying jamming nodes that mixes in with the signals. The advantages of using FJ are that in contrast to cryptographic techniques it is not computationally heavy, and it is less complex. Afaq et al [91] summarizes the use of FJ by explaining that "unlike resource- intensive centralized cryptographic approaches, FJ schemes proffer a more suitable solution for resource-constrained end devices in a distributed environment. FJ signals are introduced to suppress the decoding capability of adversaries who maliciously eavesdrop".

8.4 Secure 5G in Internet Edge

The internet Edge or the perimeter of the 5G core network refers to the access networks of various public land mobile networks (PLMNs). PLMN is typically the network of a service provider on a per country basis. It is responsible for providing the users and their UE with services such as being able to reach emergency services, make phone calls, write text messages, and send multimedia messages. These networks also function as the door or gateway to the 5G core network.

For communication channels in the NR of the 5G network, one strives to improve on throughput, latency and reliability capabilities compared to the previous 4G system. This pertains to the usage scenarios in 5G on enhanced mobile broadband (eMBB), URLLC and massive machine type communication (mMTC). This prompted the 3GPP to replace the channel-coding used in the 4G LTE such as convolutional and Turbo codes, with low-density parity check (LDPC) codes and polar codes for 5G [96].

8.4.1 Side-channel attacks

[97] highlights the challenges in relation to channel-coding in the 5G communication landscape. Specifically, side-channel attacks stand out as a prime attack method. The researchers describe side-channel attacks as "one of the methods used to recover the message from communication processes by using side-channel information" [97]. The information used to conduct such attacks are elements like time attacks, electromagnetic fields, and power consumption. The researcher's suggestion to improve on the security of side-channel attacks in the 5G network in relation to the communication channel

aspect, is a multiplicative masking method for LDPC codes which is one of the main channel-coding techniques in 5G. The foundation for carrying out the research was to use field-programmable gate arrays (FPGAs). The masking method consisted of three steps. Step one is a proposal on a multiplication algorithm in finite fields for LDPC codes. The next step is securing the LDPC codes through a multiplicative masking method based on a multiplication algorithm. It is focused on making it more difficult for attackers to derive and compute the secret key from the communication processes through side-channel attacks. It is made more difficult because the proposed method increases the randomness of the computations. In the final step, a secure coding method is proposed building on the contribution from the previous step, the multiplicative masking method. The effect of noise on information in the transmission channel is negated by encoding the data to be sent before transit. In addition, the data must be encrypted. The encoding of the LDPC codes is carried out with Gaussian elimination that does computations using inversions, additions, and multiplications. The scenarios in which LDPC codes are encoded with additions and multiplications only, are vulnerable to side-channel attacks because they are two-operand operations. The masking method proposed in this paper helps to mitigate this problem and further increase communication channel security in the 5G.

Another study looks at side-channel attacks in relation to paging. Hussain et al [98] shows that when a UE is connected to a base station but is only passively listening (i.e., not doing any tasks), the UE enters an idle state characterized by preserving power. While this connection is passive and only kept alive, at various points in time will the UE wake up from its slumber. This is referred to as the paging occasion and is best described as when "A UE in idle state wakes up periodically to check whether there is a paging message. If there is a paging message, the UE iterates over the paging records in the message while searching for its paging identity (IMSI or TMSI). It re-establishes connection with the base station if it finds its identity. The paging protocol ensures that when a base station sends a UE's paging record at a given time, the UE also wakes up at that time to check, i.e., a base station and a UE must agree on when to send/receive paging records for the UE." [98]. The determining factor on whether a paging message is present or not at the time of the paging occasion in the UE is the mobility management entity (MME).

This is a key control node that helps with managing UE access network and mobility. The entity authenticates UE and generates and distributes temporary identities to connected UE. It enables the UE to become part of the appropriate PLMN. It also conducts exchangeability across other access network technologies such as 2G and 3G [99]. Where Samaoui [99] and Hussain [98] speaks of the MME, it is primarily 4G LTE-centered. The equivalent to the MME in the 5G architecture is the Access and Mobility Management Function (AMF). The AMF is responsible for paging the UE when it is in an idle mode in 5G [100]. It determines if a particular UE is registered in a selected PLMN with RM-DEREGISTERED (not registered with the network) and RM-REGISTERED (registered with the network). If the UE is RM-REGISTERED, the AMF holds information on the routing to, and location of the UE [100]. A UE can assume two states regarding whether it is currently actively communicating with the AMF, a CM-IDLE state (meaning it currently does not have a form of NAS signaling with the AMF) and a CM-CONNECTED state (meaning it currently has some form of NAS signaling with the AMF). If the UE is registered on the network, and in a CM-IDLE state, the UE shall respond to paging by performing a so-called Service Request procedure [100]. This Service Request procedure is used both to establish a secure connection between the AMF and the UE, and for the UE to respond to a paging request and perform the paging occasion previously mentioned [101].

As can be seen when returning to the description of the paging occasion in the study of Hussain et al

[98], the International Mobile Subscriber Identity (IMSI) or Temporary Mobile Subscriber Identity (TMSI) is distributed to the UE. The IMSI is unique for the UE and is related to the SIM-card of the UE where it is stored and usually not subjected to change. The TMSI identity is generated in a random manner and assigned to the UE by the AMF. These are retransmitted in the paging information when the AMF asks the base stations related to the UE to broadcast a paging message due to services pending to communicate with the UE. These services could a be a phone call, SMS messages or services from the internet e.g., instant messaging applications. By performing multiple requests which prompts multiple pending services to be transmitted from the AMF to the UE, side-channel information such as the TMSI can show up frequently enough for the attacker to deduce that the target UE is present. The study shows that the attack can be carried out due to the synchronization of the device and the base station which it is connected to. A device contains a Paging Frame Index (PFI) that is determined by the IMSI of the device. The LTE protocol for paging events uses a set cycle. The UE only wakes up only once per LTE protocol cycle. All the paging messages during this cycle is broadcasted from the base station to the UE and its PFI serving as the reference point for all subsequent frames handling these paging messages. This can be abused when making a high number of requests or calls to the UE by looking at the amount of activity in PFIs to determine which PFI is the busiest, and with a high degree of likelihood identifying the PFI of the victim. To identify the PFI of the victim's UE means that the attacker can be assured that the victim UE is present in the cell area of interest. The researchers outline three different attack methods, each of which builds upon the previous one. These are the TORPEDO, PIERCER, and IMSI-Cracking attack. The TORPEDO attack serves as the foundation for launching the other two attacks and can be used for both the 4G and 5G technology. Using TORPEDO, an attacker can gain access to and control the paging channel of a victim. Being in possession of the paging channel, the attacker could then proceed to launch denial-of-service attacks on the UE by injecting and delivering paging messages with no content. This in turn will deny services for the UE because it will have trouble receiving legitimate paging requests from the AMF. Privacy-wise, the TORPEDO attack may have the ramifications of leading to privacy issues for the UE because it can potentially be linked to a cellular area, and because it also may detect whether the connection status between the UE and the AMF or base station is connected or idle, meaning whether it is actively communicating with the network or not. Lastly, a successful TORPEDO attack may be used to mount the other two attacks.

To mitigate or completely avoid these attacks, the TORPEDO attack is the most important one to address because without it, the other two cannot be launched. The researchers include in their study multiple suggestions on how to mitigate or thwart the attack [98]. One option is to make the fixed paging occasion non-abusable or at least limit the potential to abuse it on the level of the protocol, for example by letting the paging occasion take place through TMSI instead of IMSI. Another is to establish the signature with machine learning and deep packet inspection for the TORPEDO attack and to detect this signature. These options are however deemed infeasible to deploy by the researchers. The alternative then is what the researchers refer to as a noise-based countermeasure. This involves raising the paging rate of base stations or gNodeBs to a level that makes it quite difficult for an attacker to single out a UE from other UEs in the cellular area, providing such an amount of noise in the side-channel information that the attacker will be unable to gather information accurately enough.

8.5 Conclusion

Several issues and details on how they can be abused by adversaries have been identified in this paper. In addition, strategies, or measures to negate the effect of potential attacks have been presented. Side-channel attacks were looked at where data is analyzed and interpreted by the adversary. To thwart these kinds of attacks, a masking method and raising the frequency of paging occasions was suggested as possible solutions. For securing a continuity in real-time application of 5G, federated learning which is a technique in machine learning was suggested, and friendly jamming to confuse eavesdropping adversaries. There are likely many other ways in which to address the same issues.

Future research should be conducted to address many other issues that most certainly will be present at points during the lifecycle of 5G. The research will contribute to the continual quest for security and privacy assurance for businesses and end users while using 5G.

CHAPTER NINE

SOFTWARE DEFINED NETWORK AND SECURITY

CHAPTER

TEN

SUMMARY: ACTIONS TO BE TAKEN FOR NEXT GENERATION NETWORKS

10.1 Introduction

In the previous chapters you have hopefully garnered an overview of the technologies that will make up the next generation network. In addition to this, we have given an overview of some of the main security considerations in relation to both 5G and IPv6. As mentioned in those chapters, they are not to be seen as a complete summary of all the security consideration, as that is too comprehensive for the size and scope of this project, but rather as a good starting point for the topic. This last chapter aims to give a recommendation summary based on the preceding chapters with actions to be taken for the next generation network.

10.2 5G

In Chapter 4 we introduced 5G and the different services it will have, and the author of that chapter also gave a high-level overview of the security mechanisms described in the 3GPP standard. We acknowledged that some of the security mechanisms in the standard stem from mechanisms developed for previous generations like 4G, but that there of course has been a surge of innovation giving rise to new security mechanisms in the fields of encryption, authentication, and user privacy. We will briefly go through some of these and discuss them in relation to the risk analysis from Chapter 7. It is, however, important to note that although these new security mechanisms are excellent for their purpose, they remain only part of a much larger picture that comprises the complete security landscape. Some security features are dependent on the actual deployment and implementation and are not part of the 3GPP standard [57], like for instance a DDoS attack.

Some of the security services provided by the 3GPP standard and mentioned in Chapter 4 include mutual authentication. Mutual authentication means that both the end-user as well as the network authenticate themselves. This ensures accountability and among other things gives the service provider or the network operator the ability to lawfully intercept communications if there is legal reason to do so.

The 3GPP standard for 5G ensures that appropriate algorithms choices are made for encryption and integrity protection. They do this by employing a team of security algorithm experts of ETSI (European Telecommunications Standards Institute). The standard also ensures confidentiality of user plane data by encrypting the end-user data while it passes the network. This combats threats of eavesdropping for the waves over the air or directly from the wires. It is again important to emphasise that this mechanism only ensures confidentiality while the data is still on the network, but not when it travels to the internet – that is the responsibility of the application provider that the user is communicating with.

The last security service mentioned in Chapter 4 is compartmentalization. The purpose of this security function is to reduce the impact of a security breach. The 5G system will have different types of compartmentalization. They make it so that the breach remains contained in the specific compartment it originated from and prevents it from spreading and expanding to other compartments and as such have greater impact. One type of such a function is the compartmentalization of the RAN (Radio Access Network) and the core network functions. If a RAN was supposedly compromised and breached it would not result in that breach making its way to the core network that handles even more sensitive data than the RAN.

As mentioned earlier, these security mechanisms intend to secure data while it is still on the 5G network and not while they travel to the internet. It is the job of the application provider to configure their application in a way that complements the security the end-user is provided while on the 5G network. Which brings us to the findings of Chapter 7 where we have done a risk analysis of the 5G network and identified several high-risk incidents that need to be addressed. Keep in mind that the risk analysis is a high-level one and that it reflects the opinion of the author.

We discovered that most of these high-risk incidents would be caused by poor configuration and management rather than a limitation of the 5G security capabilities. Risk 4 mentioned in Chapter 7 is one such risk that exploits poor management wherein the organization has a poor ISSP (Information Systems Security Policy) or lacks one completely. Another one is risk 10, where an adversary breaches a single node and gets access to every asset related to the MNO (Mobile Network Operator). This kind of attack would most likely be due to poor configuration by the MNO and could perhaps be avoided by utilizing the compartmentalization functions provided by the 5G standard mentioned above. The final risk of this type is risk 11, where the adversary exploits poor access control and steals sensitive data.

What these high-risk incidents suggest, along with the security services outlined above, is that proper configuration combined with sound management still play a major role in the security industry despite technological innovation. On one hand we have several new technological innovations related to the security of 5G and on the other hand we have several high-risk incidents caused by poor management and configuration and not technological limitations. It is conceivable that as security technology advances, more risks will be due to these factors rather than technological limitations. It will remain to be seen how this will play out in the years to come as SA 5G is rolled out.

10.3 IPv6

In chapter Chapter 2 we introduced some of the key aspects that make IPv6 different from IPv4. First and foremost is the larger address space of IPv6. The second aspect was that the header format is simpler than IPv4's header format in order to reduce the processing required for packet handling. IPv6 has introduced extensions to address authentication, data integrity, confidentiality, and privacy concerns. In terms of authentication the protocol uses the IP Authentication Header (AH). In addition to this it also uses IP Encapsulating Security Payload (ESP) to ensure the protection of traffic is conforming to the CIA triad as long as these headers are included. The AH and ESP are part of the IPSec protocol suite that allows for this secure communication on the IP layer. It should be noted that these are mandatory when implementing IPv6 [11].

As IPv6 adoption continues to grow, the probability of security issues arising becomes higher. Some of these security issues stem from IPv4, but IPv6 does of course introduce new security issues. One such security issue that was a big problem in IPv4 and still somewhat relevant for IPv6 is network reconnaissance. Although this is considerably easier to do on an IPv4 network partly due to the smaller address space, it is still possible on IPv6 despite the considerably larger address space [71].

Another security challenge with IPv6 is the possibility to correlate the user's activity over time. Chapter 6 shows that this can happen when the IPv6 addresses are misconfigured. This is because IEEE-based IIDs the lifetime of the address is identical to the lifetime of the network interface. In most cases this reflects the lifetime of the device itself. An adversary can therefore use non-changing addresses as identifiers to correlate nonrelated activities across networks [73]. The challenge with this is that the address is required and cannot be encrypted or hidden easily. This challenge is unique to IPv6 as IPv4 addresses are changed more often when moving between networks.

Another challenge with IPv6 is related to the functionality of router advertisements (RAs). These are used to enable auto-configuration by letting the router periodically send information about the prefixes and the parameters on the local network. If this is configured poorly, or simply due to an adversary, then false RAs may be sent out to the link. These are called Rogue RAs and can disrupt the network partly because the prefix for the local network is derived from the RA. Several mitigation methods exist to circumvent these attacks like RAGuard and SEcure Neighbour Discovery (SEND) as mentioned in chapter Chapter 6 and in RFC 6104 [**rfc6104**].

10.4 Conclusion

The sentiment that several of these security challenges are due to misconfiguration is apparent as seen above in the previous subchapter on 5G as well as this subchapter about IPv6. It is therefore our recommendation that the configuration process when setting up these technologies gets the appropriate time and resources it deserves in order to prevent attacks. Please note that this is not a complete overview of the security challenges in 5G and IPv6 as there are many more challenges that are not mentioned here at all. This paper aims to serve as a preliminary look on these challenges to give the reader a basic overview of some of the most common security challenges to consider. Regarding topics for further reading, we would recommend IPv4 and IPv6 dual stacking due to the fact that these two protocols are set to work together for the foreseeable future until the transition to IPv6 is complete.

BIBLIOGRAPHY

[1] 2021. 5g standalone update: executive summary - june 2021. (June 2021). https://gsacom.com/paper/5g-standalone-update-executive-summary-june-2021/.

[2] Scott O. Bradner and Allison J. Mankin. 1995. The Recommendation for the IP Next Generation Protocol. RFC 1752. (January 1995). DOI: 10.17487/RFC1752. https://rfc-editor.org/rfc/rfc1752.txt.

[3] Scott O. Bradner and Allison J. Mankin. 1993. IP: Next Generation (IPng) White Paper Solicitation. RFC 1550. (December 1993). DOI: 10.17487/RFC1550. https://rfc-editor.org/rfc/rfc1550.txt.

[4] Dr. Steve E. Deering and Bob Hinden. 2017. Internet Protocol, Version 6 (IPv6) Specification. RFC 8200. (July 2017). DOI: 10.17487/RFC8200. https://rfc-editor.org/rfc/rfc8200.txt.

[5] Dr. Steve E. Deering and Bob Hinden. 2006. IP Version 6 Addressing Architecture. RFC 4291. (February 2006). DOI: 10.17487/RFC4291. https://rfc-editor.org/rfc/rfc4291.txt.

[6] 1981. Internet Protocol. RFC 791. (September 1981). DOI: 10.17487/RFC0791. https://rfc-editor.org/rfc/rfc791.txt.

[7] Shane Amante, Jarno Rajahalme, Brian E. Carpenter, and Sheng Jiang. 2011. IPv6 Flow Label Specification. RFC 6437. (November 2011). DOI: 10.17487/RFC6437. https://rfc-editor.org/rfc/rfc6437.txt.

[8] Shane Amante and Brian E. Carpenter. 2011. Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels. RFC 6438. (November 2011). DOI: 10.17487/RFC6438. https://rfc-editor.org/rfc/rfc6438.txt.

[9] Stephen Kent. 2005. IP Authentication Header. RFC 4302. (December 2005). DOI: 10.17487/RFC4302. https://rfc-editor.org/rfc/rfc4302.txt.

[10] Stephen Kent. 2005. IP Encapsulating Security Payload (ESP). RFC 4303. (December 2005). DOI: 10.17487/RFC4303. https://rfc-editor.org/rfc/rfc4303.txt.

[11] Karen Seo and Stephen Kent. 2005. Security Architecture for the Internet Protocol. RFC 4301. (December 2005). DOI: 10.17487/RFC4301. https://rfc-editor.org/rfc/rfc4301.txt.

[12] Ralph Droms. 1997. Dynamic Host Configuration Protocol. RFC 2131. (March 1997). DOI: 10.17487/RFC2131. https://rfc-editor.org/rfc/rfc2131.txt.

[13] Tomek Mrugalski, Marcin Siodelski, Bernie Volz, Andrew Yourtchenko, Michael Richardson, Sheng Jiang, Ted Lemon, and Timothy Winters. 2018. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 8415. (November 2018). DOI: 10.17487/RFC8415. https://rfc-editor.org/rfc/rfc8415.txt.

[14] Dr. Thomas Narten, Tatsuya Jinmei, and Dr. Susan Thomson. 2007. IPv6 Stateless Address Autoconfiguration. RFC 4862. (September 2007). DOI: 10.17487/RFC4862. https://rfc-editor.org/rfc/rfc4862.txt.

[15] Bob Hinden. 1998. IP Version 6 Addressing Architecture. RFC 2373. (July 1998). DOI: 10.17487/RFC2373. https://rfc-editor.org/rfc/rfc2373.txt.

[16] William A. Simpson, Dr. Thomas Narten, Erik Nordmark, and Hesham Soliman. 2007. Neighbor Discovery for IP version 6 (IPv6). RFC 4861. (September 2007). DOI: 10.17487/RFC4861. https://rfc-editor.org/rfc/rfc4861.txt.

[17] 2014. *Ipv6 the big picture*. *Practical IPv6 for Windows Administrators*. Apress, Berkeley, CA, 1–6. ISBN: 978-1-4302-6371-5. DOI: 10.1007/978-1-4302-6371-5_1. https://doi.org/10.1007/978-1-4302-6371-5_1.

[18] Lars Prehn, Franziska Lichtblau, and Anja Feldmann. 2020. When wells run dry: the 2020 ipv4 address market. In *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies* (CoNEXT '20). Association for Computing Machinery, Barcelona, Spain, 46–54. ISBN: 9781450379489. DOI: 10.1145/3386367.3431301. https://doi.org/10.1145/3386367.3431301.

[19] Kjeld Borch Egevang and Paul Francis. 1994. The IP Network Address Translator (NAT). RFC 1631. (May 1994). DOI: 10.17487/RFC1631. https://rfc-editor.org/rfc/rfc1631.txt.

[20] Kjeld Borch Egevang and Pyda Srisuresh. 2001. Traditional IP Network Address Translator (Traditional NAT). RFC 3022. (January 2001). DOI: 10.17487/RFC3022. https://rfc-editor.org/rfc/rfc3022.txt.

[21] Robert Moskowitz, Daniel Karrenberg, Yakov Rekhter, Eliot Lear, and Geert Jan de Groot. 1996. Address Allocation for Private Internets. RFC 1918. (February 1996). DOI: 10.17487/RFC1918. https://rfc-editor.org/rfc/rfc1918.txt.

[22] Matt Holdrege and Pyda Srisuresh. 1999. IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663. (August 1999). DOI: 10.17487/RFC2663. https://rfc-editor.org/rfc/rfc2663.txt.

[23] Simon Perreault, Ikuhei Yamagata, Shin Miyakawa, Akira Nakagawa, and Hiroyuki Ashida. 2013. Common Requirements for Carrier-Grade NATs (CGNs). RFC 6888. (April 2013). DOI: 10.17487/RFC6888. https://rfc-editor.org/rfc/rfc6888.txt.

[24] Sheng Jiang, Brian E. Carpenter, and Dayong Guo. 2011. An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition. RFC 6264. (June 2011). DOI: 10.17487/RFC6264. https://rfc-editor.org/rfc/rfc6264.txt.

[25] Mohamed Boucadair, Mat Ford, Phil Roberts, Alain Durand, and Pierre Levis. 2011. Issues with IP Address Sharing. RFC 6269. (June 2011). DOI: 10.17487/RFC6269. https://rfc-editor.org/rfc/rfc6269.txt.

[26] Robert T. Braden. 1992. TIME-WAIT Assassination Hazards in TCP. RFC 1337. (May 1992). DOI: 10.17487/RFC1337. https://rfc-editor.org/rfc/rfc1337.txt.

[27] Jakub Czyz, Mark Allman, Jing Zhang, Scott Iekel-Johnson, Eric Osterweil, and Michael Bailey. 2014. Measuring ipv6 adoption. *SIGCOMM Comput. Commun. Rev.*, 44, 4, (August 2014), 87–98. ISSN: 0146-4833. DOI: 10.1145/2740070.2626295. https://doi.org/10.1145/2740070.2626295.

[28] 2017. The ipv6 internet: an assessment of adoption and quality of services. *Journal of international technology and information management.*, 26, 2, 48. ISSN: 1543-5962.

[29] Google. 2021. Ipv6 adoption. Retrieved 10/26/2021 from https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption.

[30] Wang Jianing, Zhang Shilong, and Jiang Nannan Sun Lurong. 2020. Research and application of related technologies of new generation network communication protocol ipv6. In *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, 2210–2214. DOI: 10.1109/ICMCCE51767.2020.00479.

[31] Xuequn Wang and Sebastian Zander. 2018. Extending the model of internet standards adoption: a cross-country comparison of ipv6 adoption. *Information & Management*, 55, 4, 450–460. ISSN: 0378-7206. DOI: https://doi.org/10.1016/j.im.2017.10.005. https://www.sciencedirect.com/science/article/pii/S0378720616304487.

[32] Merriam-Webster. 2021. Definition of internet of things. Retrieved 10/28/2021 from https://www.merriam-webster.com/dictionary/Internet%5C%20of%5C%20Things.

[33] 2013. The future internet : future internet assembly 2013: validated results and new horizons. eng. Berlin, Heidelberg, (2013).

[34] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The internet of things: a survey. *Computer Networks*, 54, 15, 2787–2805. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2010.05.010. https://www.sciencedirect.com/science/article/pii/S1389128610001568.

[35] Kinza Shafique, Bilal A Khawaja, Farah Sabir, Sameer Qazi, and Muhammad Mustaqim. 2020. Internet of things (iot) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5g-iot scenarios. *Ieee Access*, 8, 23022–23040.

[36] Shadi Al-Sarawi, Mohammed Anbar, Rosni Abdullah, and Ahmad B. Al Hawari. 2020. Internet of things market analysis forecasts, 2020–2030. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 449–453. DOI: 10.1109/WorldS450073.2020.9210375.

[37] Curtis M Keliiaa. 2019. 5G and IPv6: Changing the Cyber-Ecosystem. Technical report. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[38] Evans Kiptoo Bartocho. 2018. *IP addressing, transition and security in 5G networks*. Master's thesis. University of Cape Town.

[39] Chris Hoffman. 2020. What is 5g, and how fast will it be? Accessed 17-Oct-2021. (January 2020). https://www.howtogeek.com/340002/what-is-5g-and-how-fast-will-it-be/.

[40] GSMA's 5G task force. 2019. The 5g guide, a references for operators. Accessed 26-Sep-2021. (2019). https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf.

[41] Wesley Chai and Corinne Bernstein. 2021. 3rd generation partnership project. Accessed 17-Oct-2021. (March 2021). https://www.techtarget.com/searchnetworking/definition/3rd-Generation-Partnership-Project-3GPP.

[42] Juan Pedro Tomás. 2021. Global 5g connections to reach 1.8 billion by 2025: gsma. Accessed 15-Oct-2021. (June 2021). https://www.rcrwireless.com/20210630/5g/global-5g-connections-reach-1-billion-2025-gsma#prettyPhoto.

[43] Telenor. 2021. Vi bygger ut 5g. Accessed 12-Oct-2021. (2021). https://www.telenor.no/dekning/5g/.

[44] Telia. 2021. Alt du vil vite om telia-nettet. Accessed 12-Oct-2021. (2021). https://www.telia.no/nett/.

[45] Global Mobile Suppliers Association. 2019. Lte and 5g market statistics – 8 april 2019. Accessed 12-Oct-2021. (2019). https://gsacom.com/paper/lte-5g-market-statistics-8-april-2019/.

[46] Amy Nordrum and Kristen Clark. 2017. Everything you need to know about 5g. Accessed 2-Nov-2021. (2017). https://spectrum.ieee.org/everything-you-need-to-know-about-5g.

[47] Jung Hyun Bae, Ahmed Abotabl, Hsien-Ping Lin, Kee-Bong Song, and Jungwon Lee. 2019. An overview of channel coding for 5g nr cellular communications. *APSIPA Transactions on Signal and Information Processing*, 8, e17. DOI: 10.1017/ATSIP.2019.10.

[48] Qualcomm. 2021. Everything you need to know about 5g. Accessed 17-Oct-2021. (May 2021). https://www.qualcomm.com/5g/what-is-5g.

[49] Aisha Javed. 2019. 5g technology – the future of connectivity. Accessed 20-Nov-2021. (June 2019). https://www.xorlogics.com/tag/5g-technology/.

[50] Mike Moore. 2019. What is industry 4.0? everything you need to know. Accessed 2-Nov-2021. (November 2019). https://www.techradar.com/news/what-is-industry-40-everything-you-need-to-know.

[51] Nick Koiza. 2021. Are 5g networks a game changer for mission-critical communications? (February 2021). https://www.rrmediagroup.com/Features/FeaturesDetails/FID/1045.

[52] GSMA. 2017. Cellular vehicle-to-everything (c-v2x). Accessed 6-Oct-2021. (December 2017). https://www.gsma.com/iot/wp-content/uploads/2017/12/C-2VX-Enabling-Intelligent-Transport_2.pdf.

[53] Marco Contento. 2020. Massive iot and 5g: what's next for large-scale cellular iot. Accessed 2-Nov-2021. (September 2020). https://www.telit.com/blog/massive-iot-5g-whats-next/.

[54] Michael Andersson, A. Özçelikkale, Martin Johansson, U. Engström, Andrei Vorobiev, and Jan Stake. 2016. Feasibility of ambient rf energy harvesting for self-sustainable m2m communications using transparent and flexible graphene antennas. *IEEE Access*, 4, (January 2016). DOI: 10.1109/ACCESS.2016.2604078.

[55] Catherine Sbeglia. 2021. What is 5g network slicing and what does it mean for enterprise 5g adoption? Accessed 12-Oct-2021. (August 2021). https://www.rcrwireless.com/20210820/5g/what-is-5g-network-slicing-and-what-does-it-mean-for-enterprise-5g-adoption.

[56] Catherine Sbeglia. 2020. Samsung, kddi demo 5g end-to-end network slicing. Accessed 17-Oct-2021. (September 2020). https://www.rcrwireless.com/20200924/carriers/samsung-kddi-demo-5g-end-to-end-network-slicing.

[57] Ericsson. 2018. A guide to 5g network security. Accessed 26-Sep-2021. (December 2018). https://www.ericsson.com/48fcab/assets/local/news/2018/10201291-04_gir_report_broschure_dec2018_webb_181212.pdf.

[58] GSMA. 2021. Network equipment security assurance scheme (nesas). Accessed 3-Nov-2021. (2021). https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

[59] LoRa Alliance. 2021. What is lorawan. (2021). https://lora-alliance.org/about-lorawan/.

[60] Semtech. 2021. What is lora? (2021). https://www.semtech.com/lora/what-is-lora.

[61] Semtech. 2021. Ulike nettverksteknologier som muliggjør iot. Accessed 14-Nov-2021. (2021). https://www.telenor.no/bedrift/iot/iot-nettverksteknologi/.

[62] Phillip Tracy. 2016. Inside iot network rollouts: lora, sigfox and lte-m. Accessed 20-Nov-2021. (July 2016). https://www.rcrwireless.com/20160715/internet-of-things/iot-network-rollouts-tag31-tag99.

[63] María Hernández. 2018. Connectivity now and beyond; exploring cat-m1, nb-iot, and lpwan connections. (July 2018). https://ubidots.com/blog/exploring-cat-m1-nb-iot-lpwan-connections.

[64] Telia. [n. d.] Massive iot - nb-iot & lte-m. Accessed Dec-2021. (). https://www.telenor.no/bedrift/iot/iot-nettverksteknologi/.

[65] Semtech. 2021. Why lora? Accessed Nov-2021. (2021). https://www.semtech.com/lora/why-lora.

[66] Remi Lorrain. 2021. The future of 5g and lorawan: friends or foes? Accessed Dec-2021. (November 2021). https://blog.semtech.com/the-future-of-5g-and-lorawan-friends-or-foes.

[67] Inpixon. 2021. Chirp spread spectrum. Accessed Dec-2021. (2021). https://www.inpixon.com/technology/standards/chirp-spread-spectrum.

[68] Actility Gemalto and Semtech. 2017. Lorawan security whitepaper. Accessed Dec-2021. (2017). https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf.

[69] LoRa Alliance Technical Committee. 2021. Lorawan is secure (but implementation matters). Accessed Dec-2021. (2021). https://lora-alliance.org/resource_hub/lorawan-is-secure-but-implementation-matters/.

[70] Agustin Pelaez. 2020. Lorawan vs nb-iot: a comparison between iot trend-setters. (February 2020). https://ubidots.com/blog/lorawan-vs-nb-iot.

[71] Chris Grundemann. 2017. Ipv6 security myth #4 - ipv6 networks are too big to scan. (September 2017). https://www.internetsociety.org/blog/2015/02/ipv6-security-myth-4-ipv6-networks-are-too-big-to-scan/.

[72] Siraj A. Shaikh, Howard Chivers, Philip Nobles, John A. Clark, and Hao Chen. 2008. Network reconnaissance. *Network Security*, 2008, 11, (November 2008), 12–16. doi: 10.1016/s1353-4858(08)70129-6.

[73] Dr. Thomas Narten, Richard P. Draves, and Suresh Krishnan. 2007. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941. (September 2007). doi: 10.17487/RFC4941. https://rfc-editor.org/rfc/rfc4941.txt.

[74] James Kempf, Jari Arkko, Brian Zill, and Pekka Nikander. 2005. SEcure Neighbor Discovery (SEND). RFC 3971. (March 2005). doi: 10.17487/RFC3971. https://rfc-editor.org/rfc/rfc3971.txt.

[75] Gunter Van de Velde, János Mohácsi, Eric Levy-Abegnoli, and Chip Popoviciu. 2011. IPv6 Router Advertisement Guard. RFC 6105. (February 2011). doi: 10.17487/RFC6105. https://rfc-editor.org/rfc/rfc6105.txt.

[76] 2021. Lte to 5g: june 2021 - global update. (November 2021). https://gsacom.com/paper/lte-to-5g-june-2021-global-update/.

[77] [n. d.] Dette er 5g. (). https://www.telenor.no/5g/.

[78] [n. d.] (). https://www.ericsson.com/en/mobility-report/dataforecasts/mobile-subscriptions-outlook.

[79] 2021. *Market drivers*. *5G Radio Access Network Architecture: The dark side of 5G*. Wiley-IEEE Press, 25–25.

[80] 2015. (July 2015). https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2370-2015-PDF-E.pdf.

[81] 2021. *Market drivers*. *5G Radio Access Network Architecture: The dark side of 5G*. Wiley-IEEE Press, 13–13.

[82] 2021. *5g system overview*. *5G Radio Access Network Architecture: The dark side of 5G*. Wiley-IEEE Press, 71–71.

[83] TechTarget Contributor. 2011. What is evolved packet core (epc) ? - definition from whatis.com. (January 2011). https://www.techtarget.com/searchnetworking/definition/Evolved-Packet-Core-EPC.

[84] 2021. *Market drivers. 5G Radio Access Network Architecture: The dark side of 5G*. Wiley-IEEE Press, 38–38.

[85] Kevin Flynn. 2018. A global partnership. (August 2018). https://www.3gpp.org/news-events/1975-sec_5g.

[86] 2021. 3rd generation partnership project; technical specification group services and system aspects; security architecture and procedures for 5g system (release 17). (September 2021). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.

[87] Jeffrey Cichonski, Joshua M Franklin, and Michael Bartock. 2017. NIST Special Publication 800-187 - Guide to LTE security. *NIST Special Publication*. DOI: 10.6028/NIST.SP.800-187. https://doi.org/10.6028/NIST.SP.800-187%20https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf.

[88] Mike Bartock, Jeff Cichonski, and Murugiah Souppaya. 2020. 5G Cybersecurity: Preparing a Secure Evolution to 5G. *The National Cybersecurity Center of Excellence (NCCoE)*, April, 22. http://www.nist.gov.%20https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/5G-pse-project-description-final.pdf.

[89] Mohammad Wazid, Ashok Kumar Das, Sachin Shetty, Prosanta Gope, and Joel J.P.C. Rodrigues. 2020. Security in 5G-Enabled Internet of Things Communication: Issues, Challenges and Future Research Roadmap. *IEEE Access*. ISSN: 21693536. DOI: 10.1109/ACCESS.2020.3047895.

[90] William Stalling and Lawrie Brown. 2018. *Computer Security: Principles and Practice, Global Edition*. Pearson Education Limited, 800. ISBN: 9781292220611.

[91] Amir Afaq, Noman Haider, Muhammad Zeeshan Baig, Komal S. Khan, Muhammad Imran, and Imran Razzak. 2021. Machine learning for 5G security: Architecture, recent advances, and challenges. *Ad Hoc Networks*, 123, (December 2021), 8. ISSN: 15708705. DOI: 10.1016/j.adhoc.2021.102667.

[92] Priyanka Mary Mammen. 2021. Federated Learning: Opportunities and Challenges, (January 2021), 5. arXiv: 2101.05428. https://arxiv.org/abs/2101.05428v1%20http://arxiv.org/abs/2101.05428.

[93] Mingzhe Chen, H. Vincent Poor, Walid Saad, and Shuguang Cui. 2020. Wireless Communications for Collaborative Federated Learning. *IEEE Communications Magazine*, 58, 12, (December 2020), 48–54. ISSN: 0163-6804. DOI: 10.1109/MCOM.001.2000397. arXiv: 2006.02499. https://ieeexplore.ieee.org/document/9311931/.

[94] Yalin E. Sagduyu, Tugba Erpek, and Yi Shi. 2021. Adversarial Machine Learning for 5G Communications Security. In *Game Theory and Machine Learning for Cyber Security*. Wiley, (September 2021), 270–288. DOI: 10.1002/9781119723950.ch14. arXiv: 2101.02656. https://arxiv.org/abs/2101.02656v1%20http://arxiv.org/abs/2101.02656%20https://onlinelibrary.wiley.com/doi/10.1002/9781119723950.ch14.

[95] Xuran Li, Hong-Ning Dai, Mahendra K. Shukla, Dengwang Li, Huaqiang Xu, and Muhammad Imran. 2021. Friendly-jamming schemes to secure ultra-reliable and low-latency communications in 5G and beyond communications. *Computer Standards & Interfaces*, 78, (October 2021), 12. ISSN: 09205489. DOI: 10.1016/j.csi.2021.103540. https://linkinghub.elsevier.com/retrieve/pii/S0920548921000350.

[96] Hyoungju Ji, Sunho Park, Jeongho Yeo, Younsun Kim, Juho Lee, and Byonghyo Shim. 2018. Ultra-Reliable and Low-Latency Communications in 5G Downlink: Physical Layer Aspects. *IEEE Wireless Communications*, 25, 3, (June 2018), 124–130. ISSN: 1536-1284. DOI: 10.1109/

MWC.2018.1700294. arXiv: 1704.05565. http://arxiv.org/abs/1704.05565%20http://dx.doi.org/10.1109/MWC.2018.1700294%20https://ieeexplore.ieee.org/document/8403963/.

[97] Haibo Yi. 2021. Improving security of 5G networks with multiplicative masking method for LDPC codes. *Computers and Electrical Engineering*, 95, (October 2021), 7. ISSN: 00457906. DOI: 10.1016/j.compeleceng.2021.107384.

[98] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. 2019. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. In *Proceedings 2019 Network and Distributed System Security Symposium*. Internet Society, Reston, VA, 15. ISBN: 1-891562-55-X. DOI: 10.14722/ndss.2019.23442. https://dx.doi.org/10.14722/ndss.2019.23442%20https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_05B-5_Hussain_paper.pdf.

[99] Salima Samaoui, Imen El Bouabidi, Mohammad S. Obaidat, Faouzi Zarai, and Wahida Mansouri. 2015. Wireless and mobile technologies and protocols and their performance evaluation. In *Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications*. Elsevier Inc., (April 2015), 3–32. ISBN: 9780128011584. DOI: 10.1016/B978-0-12-800887-4.00001-8.

[100] 3rd Generation Partnership Project 3GPP. 2021. Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS). (2021). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

[101] 3rd Generation Partnership Project 3GPP. 2021. Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS). (2021). https://www.3gpp.org/ftp/Specs/archive/23_series/23.502/.