VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

TECHNOLOGIE SÍTÍ 5G A JEJICH BEZPEČNOST

SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE **JAKUB KOMÁREK**
AUTHOR

BRNO 2021

Abstrakt

Práce se zaobírá technologií 5G a bezpečnostními machanizmy potřebných na její provoz.

Citace

KOMÁREK, Jakub. *Technologie sítí 5G a jejich bezpečnost.* Brno, 2021. Semestrální projekt. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce ,

Obsah

Kapitola 1

Úvod

5G je pátá generace mobilních sítí pro přenos dat. Tato technologie se v současné době již globálně instaluje a částečně se i používá. Od předchůdce (4G) se liší v násobně větší přenosové rychlosti – v současné době je uvažována rychlost 1Gbps, ale v budoucnu (cca rok 2030) se mluví až o 20Gbps. Další klíčový parametr je nízká latence – plánovaná latence je 1ms, zatím se reálná latence pohybuje řádově v několika milisekundách. Další důležitý milník, kterého je v plánu dosáhnout je kapacita počtu připojených zařízení – v plánu je jeden milion zařízení na metr čtverečních [6].

1.1 Příklady použití

V tomto odstavci shrnu technologie, které by měl podle normy obsahovat kompletní sytém 5G a jejich následné využití/použití [1].

eMBB (enhanced Mobile Broadband)

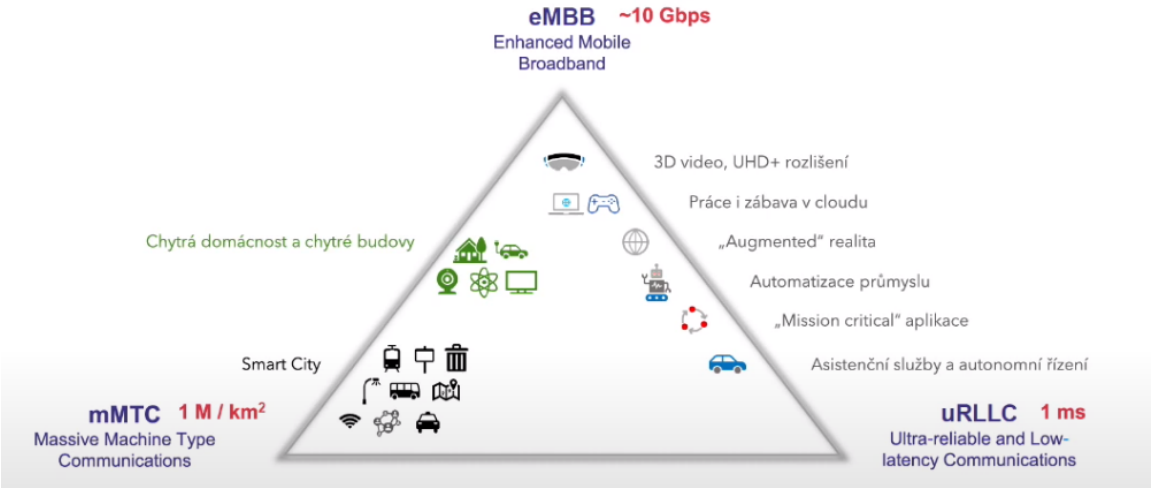
Tuto technologii využívají služby, které vyžadují velké toky dat napříč internetem. Dá se například předpokládat, že přibudou uživatelé, kteří si budou přehrávat videa/filmy ve vysoké kvalitě a tím zvýší nároky na datový provoz. Dále se očkává masivnější využívání cloud computingu. Jedná se o službu, která provádí povětšinou složité a náročné operace vzdáleně na cloudu a výsledky posílá zpátky uživateli, uživatel tedy potřebuje jen základní hardware, který slouží na zadávání požadavků a zobrazování výsledků [11]. Názorným příkladem je např. hraní her v cloudu, kdy hráč zadává instrukce, ty jsou přenášeny na server kde hra fyzicky běží a uživateli se zpátky posílá obraz se zvukem [12].

mMTC (massive Machine Type Communications)

Podstata technologie spočívá ve velkém počtu malých poměrně datově nenáročných zařízeních (Internet věcí [15]). Tyto zařízení by se mohli využít pro chytrá města či chytrá domácnost. Očekává se obrovský přírůstek těchto zařízení, proto se síť 5G dimenzuje na tyto kapacity hned od začátku [9].

URLLC (Ultra Reliable Low Latency Communications)

Uplatnění velmi nízké latence a velmi vysoké spolehlivosti by našli například služby autonomního řízení aut či jiných dopravních prostředků. Hovoří se i o vzdálených lékařských zákrocích, kdyby mohl doktor operovat vzdáleně pacienty z celého světa [9].



Obrázek 1.1: Diagram užití technologiích použitých v 5G. Získáno z [19]

1.1.1 Vize do budoucna

S příchodem 5G sítí se plánují velice ambiciózní vize. Často se tak mluví o chytrých městech, autech, silnicích atd. V případě chytrých aut se plánuje zdokonalit autonomní řízení - auta by se měla nejenom autonomně řídit, ale zároveň by měla navzájem komunikovat a sdělovat si důležité informace. Tato komunikace případně povede k lepší propustnosti silnic a k většímu bezpečí na silnici. Autonomní řízení by také hrálo velkou roli třeba v automatizaci agronomie [19].

Všechny tyto vize však potřebují pevný základ v podobě stabilní, rychlé a spolehlivé sítě, která bude mít pokrytí takřka všude. Tyto podmínky se snaží 5G sítě splnit.

Kapitola 2

Technologie

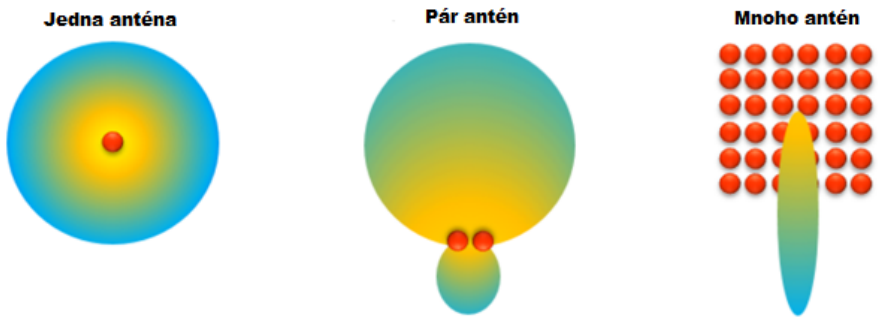
2.1 Přenosová pásma

Na rozdíl od svého předchůdce 5G využívá pro přenos signálu velkou škálu frekvencí s různými vlnovými délkami. Idea je jednoduchá – na hustě obydlené zóny budou použity krátké vlny a na např. venkov či volné prostranství budou použity dlouhé vlny. Tímto krokem dojde k co největšímu územnímu pokrytí [19].

5G bude využívat již používané frekvenční pásma mobilních sítí (2G, 3G a 4G). K těmto pásmům přibude oblast nad 700 MHz dříve okupovaná televizním signálem a nově vysokofrekvenční pásma vybraných na intervalech od 24.25 GHz do 71 GHz [16].

2.2 Paprskování (beam forming, beam steeering)

Jedná se o technologie, které umožňují cílit paprsky signálu přímo na uživatele. Základní princip funguje díky většímu množství antén, které signál posilují ve směru k uživateli a v ostatních směrech tento signál ruší. Tímto způsobem se zvýší možný počet připojených zařízení k přístupovému bodu a zároveň se navýší rychlost přenášení dat – zařízení se nebudou muset dělit o stejné frekvence [4]. Výhody této antény jsou však vykoupeny potřebným výpočetním výkonem pro provoz a řádově vyšší pořizovací cenou. Tato technika se již v malém měřítku používá v některých wi-fi přístupových bodech.

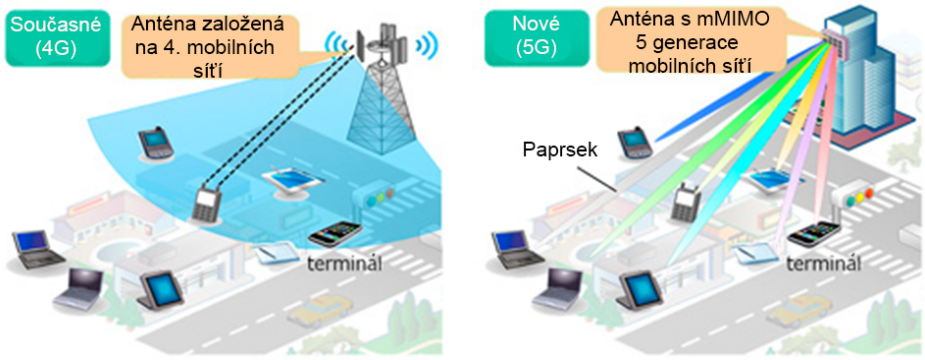


Obrázek 2.1: Demonstrace paprskování za pomocí více antén. Převzato a přeloženo z [7].

2.2.1 mMIMO

Jedná se o systém vysílací jednotky využívající výše zmíněné technologie. Zkratka mMIMO znamená „masive Multiple Input Multiple Output“. Jak již význam zkratky napovídá, jedná se o systém, který může přijímat a vysílat signál k velkému množství uživatelů v reálném čase. Anténí jednotka se skládá z logických portů. V praxi se používá 32 nebo 64 těchto logických portů. Na tyto porty připadne 128/192 fyzických antén [4].

Hmotnost hraje podstatnou roli u antény – pokud přesáhne limity dané normami pro bezpečnost práce ve výškových pracovištích, musí se antény instalovat např. jeřábem, což značně zvyšuje náklady na instalaci a údržbu. Proto se použití této technologie nejvíce vyplatí pro antény operujících na vyšších frekvencí (pro C-band). Pro antény dlouhých vln značně rostou rozměry antény a tím i hmotnost [19].



Obrázek 2.2: Na obrázku je zobrazen přenos dat na starší generací mobilní sítě v porovnání s novou. Převzato a přeloženo z [2].

2.3 Slicing

Jak bylo již zmíněno v sekci „příklady užití“ 1.1, každá služba bude mít své specifické požadavky. Proto bude možné fyzickou síť virtuálně rozdělit do více vrstev. Každá vrstva bude obsahovat pro ni potřebné technologie. Podle potřeby se pak jednotlivým vrstvám budou přiřazovat potřebné zdroje. Každá vrstva bude moci obsahovat různé úrovně zabezpečení [10] – např. síť pro monitorování počasí nebude potřebovat takovou míru bezpečnostních mechanismů jako síť určená pro provádění internetových plateb.

2.4 Infrastruktura

Pro korektní implementaci a dodržení návrhových požadavků bude potřeba modifikovat starou architekturu sítí – ve velkých městech bude potřeba násobně více antén/buněk než do posud, ty poté budou muset být propojeny optickými kabely, aby byly splněny požadavky na latenci a propustnost. Do budoucna je plánováno pokrytí vnitřku budov a přístup k síti i např. v letadle [19].

Kapitola 3

Bezpečnost

S postupem času se očekává mnohonásobně více zařízení připojených do sítě 5G. Velká část těchto zařízení však bude často primitivních/„hloupých“ typu např.: reproduktor či senzory (technologie IOT). Do posud byla tato zařízení „schována“ za routerem či firewallem a byla do jisté míry chráněná těmito prvky. S příchodem 5G se počítá s přímým napojením na tuto síť, byť tyto zařízení nemají sofistikované zabezpečení alespoň na úrovni smartphonů/-notebooků. Proto se musí zabezpečení integrovat přímo do sítě [18].

3.1 Očekávané útoky

V této sekci popíšu některé z očekávaných útoků na síť 5G a zařízení k ní připojených.

3.1.1 Dos, DDos, Botnet

Tyto útoky mají obvykle společný cíl – vždy jde o úmyslné přetížení nějaké komunikace/služby velkým počtem zbytečných požadavků. Útoky Dos jsou zpravidla vedeny z jedno počítače. DDos útoky jsou prováděny z větším počtem počítačů. Botnet je označení pro síť těchto počítačů, obvykle se útočící zařízení nedostanou do této sítě vědomě – obvykle jde o počítače napadené nějakou formou počítačového viru [5]. Tyto útoky však nejsou na poli internetu žádnou novinkou.

S příchodem 5G a jeho parametry – velmi nízkou latencí, velkou přenosovou rychlostí a velkým množstvím zařízení se tyto útoky stávají ještě nebezpečnými. A fakt že přibude více zařízeních (často nijak nechráněných) připojených do této sítě situaci nijak nevylepšuje.

Řešením je včasná detekce těchto útoků a případné odklonění v reálném čase. Do tohoto procesu by měla významně přispět umělá inteligence a strojové učení, která včas rozpozná škodlivou komunikaci a odfiltruje ji [13]. Tyto mechanismy již fungují a můžete si je pronajmou formou cloudové služby – komunikace od klientů putuje do této služby, která ji odfiltruje a přepošle směrem k vaším serverům [14]. V 5G sítích se očekává implementace těchto mechanizmů přímo do sítě.

3.1.2 Vynucená degradace komunikace

Jedná se typ útoku, kdy útočník vynutí přechod zařízení na nižší generaci sítě pomocí nějakého typu rušičky. Po tomto vynucení může útočník snáze vystopovat nebo odposlouchávat komunikaci [20].

3.1.3 Vydávání se za obslužnou síť

V těchto typech útoku se potencionální útočník vydává za legitimní obslužnou síť pro autentizaci uživatele a pokouší se při připojení zařízení na tento server odchytit důležitá data v průběhu ověření zařízení. Tento problém řeší ověřovací mechanizmy popisované v sekci 3.2 .

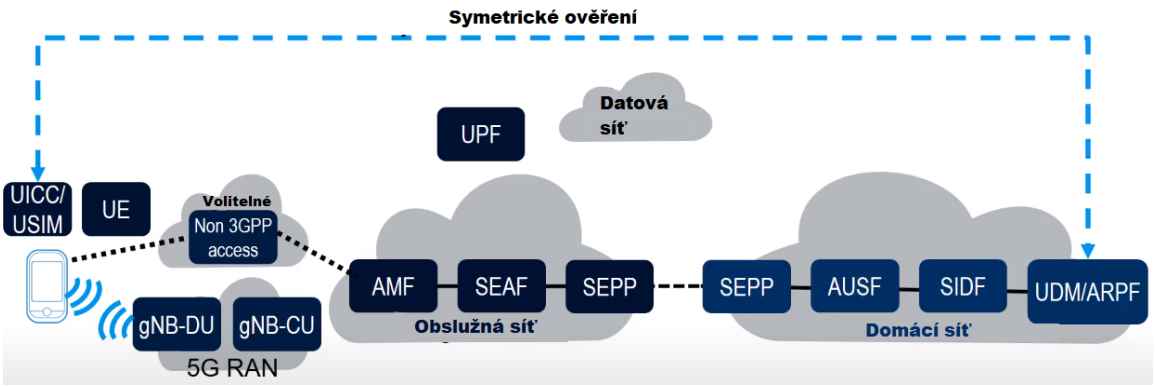
3.2 Ověření uživatele

Ačkoliv většina 5G sítí zatím fungují v hybridním módu (non-standalone) – ověření a řízení se provádí přes sítě starších generací [19], tak popíšu jak probíhá autentizace uživatele v čistě 5G síti.

Pozn.: Celá sekce čerpá z podkladů [8], [3] a [17].

3.2.1 Hlavní aktéři

- USIM – SIM karta s privátním šifrovacím klíčem. Nachází se v zařízení, které žádá o autentizaci. Stejný klíč je uložen i v jádru domácí sítě(UDM/ARPF)
- SEAF(Security Anchor Function) – Slouží jako prostředník mezi uživatelem a domovskou sítí.
- SEPP(Security Edge Protection Proxy) – slouží k zabezpečené komunikací mezi domovskou a obslužnou sítí.
- AUSF(Authentication Server Function) – Provádí autentizaci v domácí síti.
- SIDF(Subscription Identifier De-concealing Function) – Získává pravou identitu SUPI ze SUCI.
- UDM/ARPF – Repositář uložených klíčů. Funkce ARPF rozhoduje o autentizační metodě ověření.



Obrázek 3.1: Obrázek zobrazující klíčové komponenty pro autentizaci uživatele. Převzato a přeloženo z [8].

3.2.2 Autentizační zprávy

- SUPI–permanentní identifikátor klienta, je uložen na SIM kartě klienta a v repositáři domovské sítě(UDM/ARPF).
- SUCI–zašifrované SUPI. Náhradou SUCI může být dočasný identifikátor (5G-GUTI).
- Autentifikační vektor – vektor je generován v UDM/ARPF. Skládá se z AUTH tokenu, XRES tokenu a klíče K_{AUSF}.

3.2.3 Průběh ověření

Zařízení se může do sítě 5G připojit buď přímo přes síť 5G RAN nebo např. přes Wi-Fi router připojený k této síti (na obrázku 3.1 zobrazeno jako „Non 3GPP access“). V případě připojení přes zařízení které není 3GPP (např. zmiňovaný Wi-Fi router) se musí navíc mezi obslužnou sítí a zařízením vytvořit VPN tunel [3].

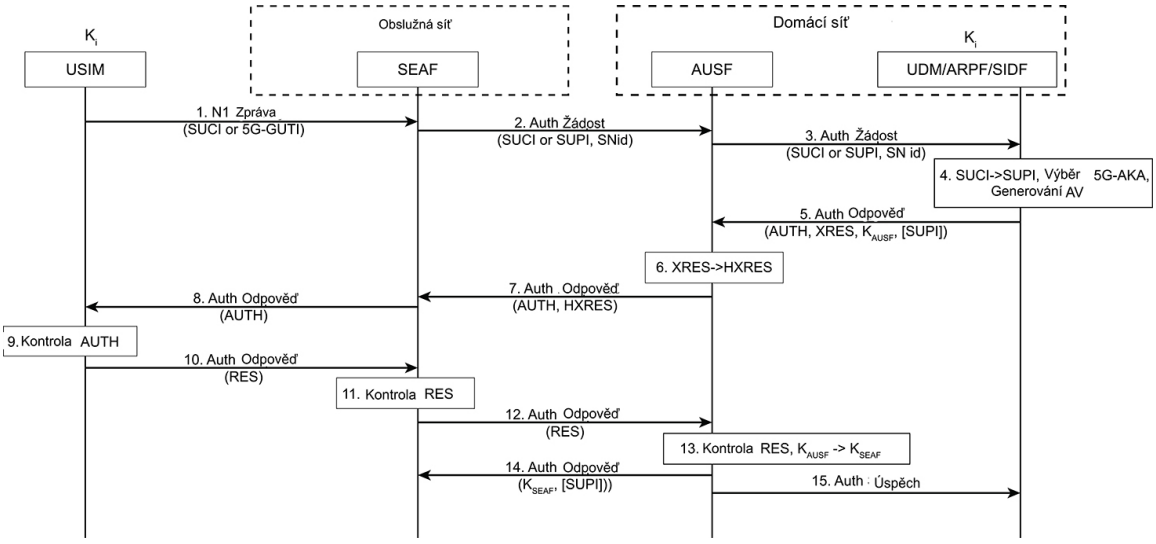
Autentizace začíná žádostí na ověření, tato žádost obsahuje SUCI a je propagovaná až do ARPF. Pokud je v UDM/ARPF záznam o daném SUCI, tak se pomocí SIDF toto SUCI rozšifruje na SUPI. Poté UDM/ARPF vybírá metodu autentizace (5G-AKA, EAP-AKA). 5G-AKA se volí v případě, kdy se musí ověřit obslužná síť, EAP-AKA je použit v případě, kdy je zaručena integrita obslužné sítě (např. je součástí domácí sítě) [8]. V situaci na popisovaném obrázku 3.2 je zvolena 5G-AKA.

Metoda 5G-AKA začíná zasláním autentizačního vektoru 3.2.2 a SUPI do AUSF. AUSF si uloží klíč K_{AUSF} a spočítá HXRES. Poté zasílá token AUTH a vypočítané HXRES směrem do SEAF. SUPI se při tomto kroku neposílá, aby se zabránilo zneužití v případě zjištěné nedůvěry mezi obslužnou a domácí sítí.

SEAF si z této správy uloží HXRES a zašle do zařízení získaný token AUTH. Pomocí tajného klíče, který sdílí s domácí sítí si zařízení ověří token AUTH. Při úspěšném ověření zařízení považuje síť za autorizovanou. Po tomto ověření zasílá zařízení spočítaný RES token do SEAF. SEAF spočítá z této odpovědi HRES a porovná s uloženým záznamem.

V dalším kroku je token RES přeposlán do AUSF. Tato odpověď je porovnána s uloženým záznamem XRES. Po úspěšném ověření je vypočten K_{SEAF} a jeho derivace spolu se SUPI je odeslána zpět do SEAF. Zpráva o úspěchu je odeslána do UDM/ARPF pro účely auditu [3].

Po tomto procesu je zařízení autentizované.



Obrázek 3.2: Obrázek zobrazující průběh autentizace zařízení. Převzato a přeloženo z [3].

Kapitola 4

Závěr

Sítě 5G mají velký potenciál, využívají nejmodernější techniky a snaží se tak být co nejefektivnější. Jejich úspěch je však podmíněn zabezpečením této sítě. V případě úspěchu nabídnou zázemí pro širokou škálu služeb a techniky.

Literatura

[1] *What are eMBB, URLLC and mMTC?* [online]. Mediatek, 2018 [cit. 2021-04-20]. Dostupné z: https://www.mediatek.com/blog/5g-what-are-embb-urllc-and-mmtc.

[2] *5G Massive MIMO Testbed: From Theory to Reality* [online]. Ni, 2019 [cit. 2021-04-21]. Dostupné z: https://www.ni.com/cs-cz/innovations/white-papers/14/5g-massive-mimo-testbed--from-theory-to-reality--.html.

[3] *A Comparative Introduction to 4G and 5G Authentication* [online]. cablelabs, 2019 [cit. 2021-04-25]. Dostupné z: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication.

[4] *Beamforming & Beamsteering Antennas* [online]. Electronicsnotes, 2020 [cit. 2021-04-20]. Dostupné z: https://www.electronics-notes.com/articles/antennas-propagation/smart-adaptive-antennas/beamforming-beamsteering-antenna-basics.php.

[5] *Denial-of-service attack* [online]. Wikipedia, 2020 [cit. 2021-04-21]. Dostupné z: https://en.wikipedia.org/wiki/Denial-of-service_attack.

[6] *Everything you need to know about 5G.* [online]. Qualcomm, 2020 [cit. 2021-04-20]. Dostupné z: https://www.qualcomm.com/5g/what-is-5g.

[7] *How 5G Works* [online]. Keysight technologies, 2020 [cit. 2021-04-21]. Dostupné z: https://blogs.keysight.com/blogs/inds.entry.html/2020/08/31/how_5g_works_thedi-E9uz.html.

[8] *R&S Thirty-Five: 5G security aspects* [video]. Rohde Schwarz, 2020 [cit. 2021-04-24]. Dostupné z: https://www.youtube.com/watch?v=RgxHHqSxNlM&t=639s&ab_channel=RohdeSchwarz.

[9] *5G Applications and Use Cases* [online]. Digi, 2021 [cit. 2021-04-20]. Dostupné z: https://www.digi.com/blog/post/5g-applications-and-use-cases.

[10] *5G Network Slicing* [online]. Viavi, 2021 [cit. 2021-04-23]. Dostupné z: https://www.viavisolutions.com/es-es/node/71717.

[11] *Cloud computing* [online]. Wikipedia, 2021 [cit. 2021-04-20]. Dostupné z: https://en.wikipedia.org/wiki/Cloud_computing.

[12] *Cloud gaming* [online]. Wikipedia, 2021 [cit. 2021-04-20]. Dostupné z: https://en.wikipedia.org/wiki/Cloud_gaming.

[13] *DDoS attacks intensify — Driven in part by COVID-19 and 5G* [online]. Secutity, 2021 [cit. 2021-04-21]. Dostupné z: https://www.securitymagazine.com/articles/94570-ddos-attacks-intensify-driven-in-part-by-covid-19-and-5g.

[14] *DDoS Shield* [online]. verizon, 2021 [cit. 2021-04-21]. Dostupné z: https://www.verizon.com/business/products/security/network-cloud-security/ddos-shield/.

[15] *Internet of things* [online]. Wikipedia, 2021 [cit. 2021-04-20]. Dostupné z: https://en.wikipedia.org/wiki/Internet_of_things.

[16] Craven, C. *What Is the 5G Spectrum? Definition* [online]. sdxcentral, 2020 [cit. 2021-04-20]. Dostupné z: https://www.sdxcentral.com/5g/definitions/what-is-5g-spectrum/.

[17] Edris, E. K. K., Aiash, M. a Loo, J. K.-K. Formal Verification and Analysis of Primary Authentication based on 5G-AKA Protocol. In: *2020 Seventh International Conference on Software Defined Systems (SDS)*. IEEE, 2020, s. 256–261. ISBN 9781728172194.

[18] Harvey, P. *Avast's Sean Obrey on 5G cybersecurity for consumers* [video]. Light Reading Video, 2020 [cit. 2021-04-21]. Dostupné z: https://www.youtube.com/watch?v=0uNFVNzpFEs&ab_channel=LightReadingVideo.

[19] Holý, P. *Týden Inovací 2020: 5G sítě - budoucnost pro digitální města* [video]. CETIN, 2020 [cit. 2021-04-20]. Dostupné z: https://www.youtube.com/watch?v=-AdXpyS6eJk&ab_channel=CETIN.

[20] Kshetri, N. a Voas, J. 5G, Security, and You. *Computer (Long Beach, Calif.)*. IEEE. 2020, sv. 53, č. 3, s. 62–66. ISSN 0018-9162.