S Z A K D O L G O Z A T

Kiss Bence

2022

Nemzeti Közszolgálati Egyetem

Hadtudományi és Honvédtisztképző Kar

Híradó Tanszék

Katonai üzemeltetés szak

Híradó Szakirány

Az 5. generációs mobilhálózatok jellemzői, biztonsági aspektusai és alkalmazási lehetőségei a védelmi szférában

A konzulens:

Dr. Jobbágy Szabolcs őrnagy, adjunktus

Szakfelelős:

Dr. Farkas Tibor őrnagy, egyetemi docens

Készítette:

Kiss Bence

Budapest

2022

TARTALOMJEGYZÉK

BEVEZETŐ RÉSZ 4

A témaválasztás indoklása 4

A téma helye, szerepe, kapcsolódásai, jelentősége, aktualitása 4

Célkitűzések megfogalmazása 6

1. A MOBILHÁLÓZATOK GENERÁCIÓI – A 0G-TŐL A 4G-IG 6

1.1 A mobil rádiótelefon rendszerek 7

1.2 Az 1. generációs mobilhálózatok 8

1.3 A 2. generációs mobilhálózatok 9

1.4 A 3. generációs mobilhálózatok 12

1.5 A 4. generációs mobilhálózatok 14

1.6 Összefoglalás 16

2. AZ 5G JELLEMZŐI ÉS SAJÁTOSSÁGAI 18

2.1 Release 14 19

2.2 Release 15 22

2.3 Release 16 26

2.4 Release 17 29

2.5 Összefoglalás 31

3. AZ 5G BIZTONSÁGI KÉRDÉSEI ÉS KOCKÁZATAI 32

3.1 Felhasználói eszközök biztonsága 34

3.2 A hozzáférési hálózat biztonsága 35

3.3 A maghálózat biztonsága 36

3.4 A hálózati szeletek biztonsága 37

3.5 Az 5G biztonságával foglalkozó fontosabb jogszabályok, dokumentumok 38

3.6 Összefoglalás 40

4. AZ 5G KATONAI BEVEZETÉSÉNEK ÉS ALKALMAZÁSÁNAK LEHETŐSÉGEI 41

4.1 A NATO szövetségesek álláspontja az 5G alkalmazásának tükrében 41

4.2 Az 5G alkalmazási lehetőségei és kockázati tényezői a védelmi szféra keretein belül 43

4.3 Összefoglalás 45

BEFEJEZŐ RÉSZ 46

A téma rövid összegzése, a lényeg kiemelése 46

A témával kapcsolatos jövőbeni szándékok 47

IRODALOMJEGYZÉK 48

HIVATKOZÁSOK JEGYZÉKE 51

RÖVIDÍTÉSEK JEGYZÉKE 53

ÁBRÁK, TÁBLÁZATOK JEGYZÉKE 54

BEVEZETŐ RÉSZ

A témaválasztás indoklása

A mai modern digitális kommunikációban a mobilitás kulcsfontosságú szerepet tölt be. Az 5. generációs mobilhálózat (továbbiakban 5G) „korunk egyik legmeghatározóbb technológiai újdonsága, amely a távközlési szolgáltatások képességeinek radikális bővítése mellett merőben új innovatív szolgáltatások kialakulását segíti elő. Számos területen hoz különleges és lenyűgöző változásokat: a közlekedésben, az iparban, a mezőgazdaságban, az egészségügyben, az energiagazdálkodásban, a szórakoztatóiparban” [1] stb. érezzük vagy érezhetjük a hatását.

Ezenkívül a digitális kapcsolat központi jelentősége a Covid-19 világjárvány idején még hangsúlyosabbá vált, megvilágítva társadalmunk jelentős támaszkodását a telekommunikációs hálózatokra, valamint a digitális infrastruktúrákra és szolgáltatásokra. Ennek eredményeképpen az 5G hálózatok lehető leggyorsabb és legbiztonságosabb módon történő bevezetése kulcsfontosságú. „Az 5G-re való átállás kapujában a mobiltechnológia legalább olyan mértékű változás előtt áll, mint amit korábban a 3G-ről a 4G-re való átállás jelentett”. [2] Az átállás jelenleg is folyamatban van.

Témaválasztásom indokolja, hogy a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karán katonai üzemeltetés alapszak, híradó specializáció, információbiztonsági modulon tanulok ahol a különböző mobilkommunikációs technológiák megismerése az adott szakirány egyik legfontosabb területe. A nevezett téma nemcsak az adott szakirányt érinti, hanem többnyire egész tanulmányunkat végigköveti.

A téma helye, szerepe, kapcsolódásai, jelentősége, aktualitása

Az 5G megjelenése erős társadalmi „ellenállásba” ütközött, melyet a korábbi új technológiáknál nem tapasztaltunk. Az álhírek leginkább az 5G élettani hatásaira irányultak, melyek odáig fajultak, hogy egyes csoportok 5G tornyokat rongáltak meg. A mobilhálózatok korábbi generációit is kapcsolatba hozták a daganatos megbetegedések kialakulásával, így az 5G-t is. Az egészségügyi szervezetek folyamatosan vizsgálják a mobilhálózatok káros hatásait, melyet eddig tudományosan nem tudtak alátámasztani. Élettani hatásokkal való összefüggését mutathatja, hogy Hollandiában az egyik 5G torony tesztelése során közel 300 madár pusztult el egyszerre a torony közelében, azt azonban nem tudták megállapítani, hogy mi is okozta a madarak elpusztulását. A COVID-19 járvánnyal is összefüggésbe hozták az 5G-t, miszerint az

5G által kerül kisugárzásra a vírus, melynek persze semmi alapja nem volt, de annál nagyobb hatást ért el.

Az 5G elterjedésével az ipar komoly digitális átalakulás küszöbén áll. A különböző technológiák fejlesztés alatt állnak, vagy megjelentek már, de széles körben még nem terjedtek el. Egy gyárban a gépek, az eszközök, az emberek nagy mennyiségű adatot generálnak, melynek a kezelését, továbbítását, feldolgozását, védelmét az 5G a magas átviteli sebességének és alacsony válaszidejének köszönhetően megfelelően tudja kezelni, így az adott gyárat idő- és költséghatékonnyá alakítva át. Ez a hatékonyság megjelenik a termelésben, a felügyeletben, az irányításban, a biztonságban és a költségekben is. Legegyszerűbb példa erre a gyártási, üzemeltetési és raktározási vezeték nélküli automatizálás lehetősége, amikor a gyártást vezeték nélküli számítógép vezérelt robotok hajtják végre, a raktározást pedig emberi beavatkozás nélküli szállító egységek, targoncák végzik.

Az 5G a háztartásokban is változást fog eredményezni. Az okos otthonok jelenleg nem elterjedtek annyira, mivel az eszközök és a rendszer kialakítása költséges. Az 5G adatátviteli sebességével és rövid válaszidejével olyan hálózat hozható létre az otthonokban, melyek képesek azonnal reagálni a különböző eseményekre (pl.: hőmérsékletváltozás, áramszünet, betörés stb), így egy stabil, megbízható, sokoldalú, biztonságos környezetet kialakítva a családok számára. Mivel okos eszközöket alkalmazunk, így természetesen figyelni kell a biztonság megfelelő kialakítására.

Az 5G már olyan adatátviteli sebességgel rendelkezik, mely kiválthatja a vezetékes internet- és tévészolgáltatásokat, megtartva a vezeték által nyújtott minőséget vagy akár felül is múlva azt. A vezeték nélküliségnek köszönhetően olyan nehezebben megközelíthető területeken is elérhető lesz a minőségi szolgáltatás, ahol a vezeték kiépítése eddig gondot okozott.

A biztonság, kiberbiztonság terén a jövő telekommunikációs hálózatai új típusú megközelítést igényelnek. Az 5G hálózatok a 3G és 4G hálózatokkal ellentétben sokkal inkább célpontokká válhatnak, ugyanis a sokoldalúság miatt a sebezhetőség is fokozottabb. A távközlési infrastruktúra eddig csak transzfer szerepet játszott a kibertámadások során. Az informatikai rendszerek helyett a távközlési hálózatok is célpontok lehetnek a kiberbűnözők számára, nemzetbiztonsági és üzleti titkokhoz férhetnek hozzá. [3] A mobilhálózatok, mint vezeték nélküli hálózatok, rádióhullámok segítségével kommunikálnak így könnyebben bemérhetők, kompromittálhatók, lehallgathatók, megsemmisíthetők.

Úgy gondolom, hogy a mobilhálózatokkal kapcsolatos biztonsági szabványok, előírások elkészítése során a célok megfogalmazása, annak végrehajtási menete, technikája sok buktatót rejt magában, amely hibák elkövetése esetén a rosszul elvégzett biztonság kialakítása károsíthatja a környezetet, a szervezetet, illetve az abban dolgozó személyeket.

Megfogalmazhatók, illetve több, a témával foglalkozó kutató, szakember már meg is fogalmazta a mobilhálózatokkal kapcsolatban azokat az általános elveket, amelyek bármely szervezetre alkalmazva a biztonsági célok eléréséhez vezetnek. Ezeket az általános elveket bármely vezeték nélküli hálózat - így az 5. generációs mobilhálózat - tekintetében is figyelembe kell venni.

Célkitűzések megfogalmazása

Dolgozatomban szeretném áttekinteni és rendszerbe foglalni a mobilhálózatok generációit, beleértve a generációk történetét, szabványaikat, az előnyeit és hátrányait, továbbá a generációkban lévő kockázatokat.

Szakdolgozatomban egyszerűbb, értelmezhetőbb, de részletekbe menő ismeretet szeretnék biztosítani hallgatótársaim, illetve a dolgozatot olvasó személy számára az 5G hálózat biztonságával és annak kialakításával kapcsolatban.

Vizsgálataimmal szeretnék a dolgozatot olvasó személy számára egy olyan átfogó, minden területre kiterjedő ismeretet biztosítani a biztonság megfelelő kialakítására, melynek az alkalmazásával az új biztonsági kockázatok is kezelhetők, megoldhatók.

Mindezek mellett szeretnék képet alkotni az 5G katonai bevezetésének állapotáról a NATO tagországokban, illetve néhány, a védelmi szférában való jövőbeli alkalmazási lehetőséget is ismertetni szeretnék.

1. A MOBILHÁLÓZATOK GENERÁCIÓI – A 0G-TŐL A 4G-IG

A fejlődés az ember alkotta dolgokhoz ugyanúgy kötődik, mint a természet által létrehozottakhoz. A különbség az, hogy az ember technológiát fejleszt, a természet pedig az evolúción keresztül fejlődik. A mobilhálózatokban is megfigyelhető a technológiai fejlődés, mely fejlődés állomásait generációknak nevezzük. A generáció szó az elnevezésükben is megjelenik („G”), ami a mobiltelefon-technológia időbeli fejlődésére utal.

Mielőtt az 5. generációs mobilhálózatok biztonsági kérdéseit és specifikumait kifejteném, fontosnak tartom megismertetni a mobilhálózatok korábbi generációinak történetét, azok működését. Az elemzéshez mindenképp ajánlott megismerni a mobiltelefonos kommunikáció

működését és a generációk biztonsági kérdéseit, mivel ez esetben elengedhetetlenül szükséges egy-egy, az elemzésből levont következtetéshez.

1.1 A mobil rádiótelefon rendszerek

A mobil rádiótelefon rendszerek vezeték nélküli típusú telefonrendszerek voltak, amelyek megelőzték a telefontechnológia modern cellás mobil formáját. Mivel ezek a rendszerek a mobiltelefonok első generációjának elődei voltak, idővel ezeket visszamenőleg kezdték 0. generációs mobilhálózatoknak (0G-nek) nevezni, melyek 1946-ban, a második világháború után váltak elérhetővé kereskedelmi forgalomban. Ezek a korai mobiltelefon-rendszerek abban különböztek a korábbi zárt rádiótelefon-rendszerektől, hogy kereskedelmi szolgáltatásként a nyilvános kapcsolt telefonhálózat részeként, saját telefonszámukkal voltak elérhetőek, nem pedig egy zárt hálózat részeként.

Ezekben az eszközökben a kommunikáció eleinte csak fél-duplex vonalon zajlott, ami azt jelentette, hogy egyszerre csak egy ember beszélhetett. Az ilyen eszközök rendelkeztek egy PTT (Push to Talk) gombbal, mely megnyomásával az eszköz hangvételi módból adási módba váltott. Az eszközöket leggyakrabban személyautóba vagy teherautóba szerelték. Egyes készülékek kézi kapcsolásos rendszert használtak, azaz egy operátor segített tárcsázni és a hívást irányítani. Az eszközök analóg elven működtek.

A 0G rendszerek elég kezdetlegesek voltak, kevés csatornával és felhasználóval rendelkeztek. Ez abból adódott, hogy kevés használható frekvenciasáv volt. Kizárólag csak hang kommunikációra használták.

Néhány rádiórendszer - megjelenésük sorrendjében - röviden bemutatva:

- Mobile Telephone Service (MTS): Az egyik legkorábbi mobiltelefon szabvány. 1946-ban jelent meg az USA-ban. Ez a szolgáltatás kapcsolási rendszeren alapult, azaz a hívásokat egy operátor irányította és tárcsázta. Az MTS továbbfejlesztett változata közvetlen hívásra és full-duplex működésre volt képes.
- A-Netz: 1958-ban vezették be az NSZK-ban, és 1977-ig működött. Kézi kapcsolással működött, a készülékek rendkívül drágák és terjedelmesek voltak. A rendszer 156 MHz és 174 MHz közötti frekvencia tartományban, 10 W-os átviteli teljesítménnyel, 50 kHz csatornatávolsággal, FM modulációval működött, kb. 11000 felhasználóval. Ezt a rendszert is fejlesztették. A B-Netz 1972-től működött és már közvetlen hívást biztosított.

- System 1: A legelső nyilvános mobiltelefon-szolgáltatást az Egyesült Királyságban 1959-ben tették elérhetővé. Korlátozott kapacitású volt, és Dél-Lancashire térségében biztosított lefedettséget, kézi kapcsolással működött. A rendszer továbbfejlesztésére többször sor került egészen System 4-ig, minden fejlesztéssel tovább növelve a csatornaszámot.

Az előző rendszereken felül számos más rendszer is működött, többnyire a skandináv országokban (pl.: Mobiletelefonisystem, Offentlig Landmobil Telefoni, Autoradiopuhelin). Ezenfelül említést érdemel a Szovjetunióban működő Altaj rendszer és Csehszlovákia első hálózata, az Automated Municipal Radiotelephone is.

Ahogyan az előbbiekben láthattuk, ezek a 0G-s rendszerek eltérő specifikációk alapján működtek, nem volt kompatibilitás közöttük. Megállapítható, hogy a rendszerek kezdetlegessége és hiányosságai miatt a hívások lehallgathatósága könnyedén végrehajtható volt.

1.2 Az 1. generációs mobilhálózatok

Az 1. generációs mobilhálózat (a továbbiakban: 1G) a vezeték nélküli cellás hálózatok első generációjára utal. Az 1G megjelenése az 1970-es évek végére, az 1980-as évek elejére tehető. Ugyan a rendszer már digitális jelzést is használt a rádiótornyok összekapcsolására, de a hangátvitel analóg (FM) elven történt.

Különböző országokban különböző 1G szabványokat alkalmaztak. Az egyik ilyen szabvány az NMT (Nordic Mobile Telephone), amelyet a skandináv országokban, Kelet-Európában és Oroszországban használtak. Más szabványok közé tartozott az Egyesült Államokban használt AMPS (Advanced Mobile Phone System), az Egyesült Királyságban használt TACS (Total Access Communications System), a Japánban működő JTACS (Japan Total Access Communications System) és az NTT (Nippon Telegraph and Telephone Corporation) által kifejlesztett szabványok, a nyugat-németországi C-Netz, a francia Radiocom 2000 és az olaszországi RTMI (Radio Telefono Mobile Integrato). Ezek a szabványok a 450 MHz-es és a 900 MHz-es frekvenciatartományban működtek. Az analóg mobilszolgáltatást a legtöbb helyen fokozatosan szüntették meg világszerte. „Ezek jellemzője az volt, hogy bizonyos területeket, de maximum egy országot fedtek le, az egyes készülékek pedig kizárólag csak a saját hálózaton működtek” [4], amelyeken hangalapú közlemények voltak továbbíthatók és fogadhatók valós időben.

Az NMT specifikációk nyíltak és ingyenesek voltak, amelyek olyan gyártók elődeit segítették az eszközgyártásban, mint a Nokia, az Ericsson vagy a Motorola. Magyarországon az első mobilhálózat, három bázisállomással, Budapesten indult el 1990-ben, NMT alapokra támaszkodva. A szolgáltatást nyújtó cég a Westel Rádiótelefon Kft. volt. A magyar felhasználók körében óriási érdeklődésre tartott számot, és nagy népszerűségnek örvendett a mobiltelefonok megjelenése.

A különböző szabványokból jól látható, hogy az eltérő rendszerek között nem volt kompatibilitás, hiszen eltérő frekvenciatartományban működtek. Ezen felül az 1G technológia még számos hátránnyal rendelkezett. A lefedettség és a hangminőség gyenge volt, roaming (barangolás) támogatás a különböző szolgáltatók között nem létezett. Biztonsági kockázatként említhető, hogy a hívásokat nem titkosították, így bárki, aki rendelkezett rádiós szkennerrel, belehallgathatott a beszélgetésbe.

Ennek kiküszöbölésére például az NMT sávokat kitörölték a szkennerek tartományából, azonban egy szkenner könnyen újraprogramozható volt, és könnyedén alkalmazták a hívások lehallgatására. Későbbi NMT szabványok lehetőséget nyújtottak opcionális analóg kódolásra. Ha a bázisállomás és a mobilállomás is támogatta a kódolást, akkor a telefonhívás kezdeményezése során megállapodhattak annak használatáról. Továbbá, ha két felhasználónak volt olyan mobiltelefonja, amely támogatta a kódolást, akkor beszélgetés közben bekapcsolhatták azt akkor is, ha a bázisállomások nem támogatták. Az AMPS rendszernél a lehallgatás során egy speciális eszközzel lehetőség volt a telefon sorozatszámának és telefonszámának az elfogására, majd azt egy másik eszközre átmásolva, a klónozást végrehajtó, fizetés nélkül használhatta a telefonját. A megkárosított előfizető erről csak a következő számláján megjelenő többletköltségek alapján szerezhetett tudomást.

1.3 A 2. generációs mobilhálózatok

A mobilhálózatok 2. generációja (a továbbiakban: 2G) az 1990-es évek elején jelent meg kereskedelmi forgalomban. Míg az 1G hálózatok analóg rádiójeleket használtak, a 2G már digitális elven oldotta meg a hangátvitelt és a rendszer elemeinek egymással való kapcsolattartását. A 2G a következőkben hozott újdonságot a korábbi generációkhoz képest:

- a digitális átvitellel lehetőség nyílt titkosított kommunikációra;
- a rádióspektrum jobb kihasználásával több felhasználó beszélhetett egyszerre;
- lehetőség volt szöveges üzenet, SMS küldésére;
- adatátvitel megjelenése a kezdeti 9,6 kb/s sebességgel;

- a szabványok viszonylagos egységességével a gyártók között verseny alakult ki, melynek következményeként az árak és a telefonok méretei csökkentek.

A 2G szabványok megszüntették a korábbi szabványok, rendszerek egymással való inkompatibilitását. A világon a legelterjedtebb 2G technológia az ETSI[1] (European Telecommunications Standards Institute) által 1991-ben kifejlesztett GSM (Global System for Mobile Communication) volt. További technológiák közé tartozik az Észak-Amerikában használt IS-95 (Interim Standard 95) vagy cdmaOne és a Digital-AMPS, és a Japánban alkalmazott PDC (Personal Digital Cellular). Magyarországon a 2G szolgáltatás 1994-ben indult el a Pannon GSM-nek (későbbi Telenor) köszönhetően.

A GSM a legelterjedtebb 2G szabvány a világon, ami a 900 MHz-es és 1800 MHz-es sávokban üzemel. A 900 MHz körüli hullámok követik a föld felszínét, így ez a sáv alkalmas nagyobb terület lefedésére, illetve az átvitt jel kisebb csillapítást szenved el, aminek köszönhetően kisebb teljesítmény is elegendő a kisugárzáshoz. Az 1800 MHz-es sáv nagyobb sávszélességgel rendelkezik, azonban a hullámok rosszabb terjedési tulajdonságokkal rendelkeznek. A GSM egyik legfontosabb újítása az előfizetői azonosító modul, azaz a SIM-kártya megjelenése volt, ami tartalmazza az előfizető személyes adatait és telefonkönyvét, így készülék váltás esetén, a SIM-kártya áthelyezésével az előfizetőnek lehetősége van adatainak megtartására, másik készülékbe történő átvitelére. Habár a GSM hálózatot biztonságosnak szánták, a rendszer sebezhető a különböző típusú támadásokkal szemben, melyek a GSM-hálózat különböző részeit érhetik. A GSM rendelkezik felhasználó azonosítással és éteren keresztüli titkosítással. Számos éteren keresztüli titkosítást használ, melyek tervezése során elkövetett egyik legnagyobb hiba az volt, hogy elsősorban a titkosítási algoritmusokat igyekeztek titokban tartani, és nem nyújtották be őket felülvizsgálatra, ezért az algoritmusok kiszivárgása után a sebezhetőségek könnyen azonosíthatók voltak.

A 2G kapcsán megemlítendő a 2.5G- szabvány, a GPRS (General Packet Radio Service) és a 2.75G szabvány, az EDGE (Enhanced Data Rates for GSM Evolution). A GSM-et folyamatosan fejlesztették az évek során, ennek eredményeképpen jöttek létre ezek a generációk. A GPRS a GSM kiegészítése csomagkapcsolt átvitellel, mellyel 60-80 kb/s sebességet értek el. A klasszikus telefonhálózatok áramkörkapcsolással működtek, mely minőséget garantált a hívás felépítése és lebontása között. A csatorna csak hívás közben volt

[1] Európai Távközlési Szabványosító Szervezet egy független szabványosító szervezet az információ és kommunikáció területén.

használva. A csomagkapcsolás a számítógépes hálózatok újdonsága, mellyel az átvinni kívánt információt kisebb csomagokra, kisebb részekre bontjuk. Ennek eredménye a jobb kihasználtság, illetve segítségével nagyobb forgalom bonyolítható le, de egyes csomagok elveszhetnek az átvitel során, ezért a minőség nem garantált. A csatornát a híváson kívül is lehet használni. Az EDGE javított adatátviteli sebességet tett lehetővé (150-180 kb/s).

Mindkét fejlesztés a 3GPP-hez (3rd Generation Partnership Project) kötődik, ami innentől kezdve fontos szerepet töltött be a mobilhálózat generációkhoz kapcsolódó szabványok létrehozásában és fejlesztésében.

A 3GPP a világ különböző pontjain lévő távközlési szabványfejlesztő szervezeteket egyesíti, ezzel biztosítva a szervezetek közötti együttműködést, elősegítve a szabványok létrehozását. Az alábbi szervezeteket egyesíti a 3GPP:

- „Association of Radio Industries and Businesses (ARIB, Japán);
- Alliance for Telecommunications Industry Solutions (ATIS, USA);
- China Communications Standards Association (CCSA, Kína);
- European Telecommunications Standards Institute (ETSI, Európa);
- Telecommunications Standards Development Society (TSDSI, India);
- Telecommunications Technology Association (TTA, Dél-korea);
- Telecommunication Technology Committee (TTC, Japán)”. [5]

A projekt a távközlési hálózatok három alappillérére támaszkodva, három specifikációs csoporttal (Technical Specification Group, a továbbiakban: TSG) rendelkezik, melyek a következők:

- Radio Access Networks (a továbbiakban: RAN): felelős a hálózat és az eszközök, valamint az air-interfész specifikációiért;
- Services & System Aspects (a továbbiakban: SA): felelős a 3GPP-specifikációkon alapuló rendszerek általános architektúrájáért és szolgáltatási képességeiért, valamint a TSG-k közötti koordinációért;
- Core Network & Terminal (a továbbiakban: CT): felelős a terminál interfészek, a terminálképességek és a Core hálózat meghatározásáért.

A TSG-k további munkacsoportokból épülnek fel. Ezeknek a munkacsoportoknak köszönhetően fejlődtek a mobilhálózati technológiák. Fejlődésük útján, amikor elértek egy döntő pontig a fejlesztés eredményeképpen, az adott generációban azt nevezzük „Release”-nek,

azaz egyfajta kiadásoknak, amelyek már megvalósítható állapotot jelentenek. Valamennyi 3GPP-kiadásnál a fő hangsúly az, hogy a rendszert visszafelé és előre kompatibilissé tegyék annak érdekében, hogy biztosítsák a felhasználói berendezések zavartalan működését. A 3GPP egyszerre több kiadáson dolgozik, melynek keretében az éppen aktuális munka befejezése előtt már jóval hamarabb megkezdik a jövőbeli munkát is.

A 2G szabványokkal párhuzamosan jelent meg a TETRA (Terrestrial Trunked Radio) rendszer. A TETRA egy digitális, trönkölt, zártcélú hálózat, aminek a szabványa 1995-ben jelent meg az ETSI által kifejlesztve, kifejezetten kormányzati szervek, segélyszolgálatok részére. Magyarországon az Egységes Digitális Rádiótávközlő Rendszer (EDR) 2007-ben indult el a TETRA technológiára épülve és azt továbbfejlesztve. A TETRA összehasonlítható a GSM rendszerrel. A technológia előnyei a következők:

- megbízható, magas rendelkezésre-állású rendszer;
- alacsonyabb frekvencián működik (380-395 MHz), ennek köszönhetően nagyobb hatótávolsággal, nagyobb földrajzi lefedettséggel rendelkezik;
- létrehozható egy az egyhez, egy a többhöz, több a többhöz üzemmódok;
- támogatja a hitelesítést, az eszközök regisztrációját, az air-interfész titkosítást és végpontok közötti titkosítást;
- hálózat hiányában a mobiltelefonok közvetlen hívást használhatnak, vagy hálózati közvetítőként is üzemelhetnek;
- gyors telepítésű infrastruktúra.

A TETRA egy jobban megtervezett és hatékonyabb rendszer, mint a GSM. Ez a rendszer a megfelelő technikai megoldásokkal, kibővült szolgáltatásokkal és magas szintű rendelkezésre állásával segíti a rendvédelmi szervek működését. Ugyanakkor a szükséges biztonsági követelményeket jóval magasabb szinten és széles körben kell alkalmazni, hiszen egy hagyományos rendszerrel összehasonlítva, sokkal nagyobb biztonsági kockázatot jelenthetnek, például a Magyar Honvédség esetében, ha nem titkosított az átvitel.

1.4 A 3. generációs mobilhálózatok

A mobilhálózatok harmadik generációja a 2000-es évek elején jelent meg kereskedelmi forgalomban. A 3G kialakulása az ITU[2]-hoz (International Telecommunication Union) köthető, aminek az volt a terve, hogy a világ összes országában, egy globális frekvenciasávot jelöl ki a

[2] Nemzetközi Távközlési Egyesület különböző ajánlásokat ad ki, amelyek figyelembe vételével dolgozzák ki a távközléssel kapcsolatos szabványokat és jogszabályokat.

2000 MHz-s tartományban, ami egyetlen vezeték nélküli kommunikációs szabványt támogat. Ezt nevezzük IMT-2000 (International Mobile Telephone 2000) ajánlásnak. Míg az ITU ajánlásokat fogad el a jövőbeli globális kommunikációhoz használt technológiákra vonatkozóan, a szabványosítási vagy fejlesztési munkát azonban nem maguk végzik el, hanem más szabványosító testületek, például az IEEE (Institute of Electrical and Electronics Engineers), a WiMAX Forum és a 3GPP munkájára támaszkodnak.

Az IMT-2000 specifikációban számos olyan jellemző van meghatározva, amelyeknek az ezekre épülő technológiáknak meg kell felelniük. A fő követelmények a következők:

- legyen világszerte használható, a műholdas és a földi rendszerek integrálódjanak a globális lefedettség biztosítása érdekében;
- legyen minden rádiós környezetben használható (pl.: LAN, vezeték nélküli, cellás, műholdas);
- távközlési szolgáltatások széles skáláját nyújtsa (pl.: hang, adat, multimédia, internet);
- támogassa mind a csomagkapcsolt, mind az áramkörkapcsolt adatátvitelt;
- biztosítsa a magas adatátviteli sebességet akár 2 Mbit/s-ig, 144 kbit/s a nagy mobilitás esetében, 384 kbit/s mozgáskorlátozottan és 2 Mbit/s beltéri irodai környezetben;
- használja hatékonyan a spektrumot.

A 3G a korábbi technológiákhoz képest a következő fejlesztésekkel rendelkezik:

- jobb spektrális kihasználtság révén nagyobb hálózati kapacitás;
- nagyobb adatátviteli sebesség;
- fejlettebb és újabb szolgáltatások, mint a videohívás, internetelérés, IPTV, GPS, videokonferencia.

A GSM számára a 3G evolúció az UMTS –t (Universal Mobile Telecommunications System) eredményezte. A cdmaOne rendszerek fejlődése a CDMA2000-hez vezetett. Az UMTS a GSM hálózatokra alapozva egy komplex hálózati rendszert határoz meg. A Release 99 384 kbit/s-os sebességet ír le az első UMTS alapú rendszerekhez. Az UMTS rendszereket a roaming támogatásához is tervezték, ezen felül, ha a telefon UMTS lefedettségen kívül esik, ott a hívás átadható a GSM lefedettségnek, mivel a telefonok mindkettőt támogatják. Az interoperabilitást szem előtt tartva az UMTS telefonok több frekvenciát is támogatnak, mert különböző országok különböző frekvenciatartományokat használnak. Míg Európában a 2100 MHz-et használja, addig az USA-ban a 850 MHz-en és 1900 MHz-en működik. Ahogy látható a gyártóknak

többsávos UMTS és GSM módban kellett a telefonokat legyártani ezáltal alacsony üzemidejű készülékeket eredményezve.

Az UMTS fő vetélytársai a CDMA2000 és az EDGE. A CDMA2000 sávszélesség igénye kisebb az UMTS-nél, így a spektrumban könnyebb elhelyezni a szolgáltatóknak. Az EDGE a meglévő GSM spektrumokat használja, és telepítés szempontjából sokkal könnyebb a meglévő GSM hálózatba implementálni, mint az UMTS esetén új berendezéseket telepíteni.

A 3G szabványokat is továbbfejlesztette a 3GPP. A HSPA (High Speed Packet Access) két protokoll ötvözete, mely javítja, és kiterjeszti a 3G hálózatok teljesítményét UMTS protokollokból kiindulva. A két protokoll a le- (High-Speed Downlink Packet Access, a továbbiakban: HSDPA), illetve a felfelé irányuló (High-Speed Uplink Packet Access, a továbbiakban: HSUPA) csomagkapcsolt hozzáférést különbözteti meg. Mindkét protokoll az adatátviteli sebességet javítja, növelve a kapacitást és csökkentve a késleltetést. A HSDPA 3.5G néven is ismert, amit a 3GPP a Release 5-ben vezetett be, és 14 Mbit/s adatátviteli sebességet kívánt elérni. A HSUPA a 3.75G, melyet 3GPP a Release 6-ban specifikálta 5,76 Mbit/s adatátviteli sebességgel. További jelentős adatátviteli sebesség növekedés érhető el a HSPA+ (Evolved High Speed Packet Access) által a Release 7, 8, 9, 11-ben leírtak alapján.

A 3G hálózatok nagyobb biztonságot nyújtanak, mint a 2G elődeik. Az UMTS hozzáférési biztonsági szabványok új hitelesítési mechanizmuson alapulnak, amelyek kiterjednek az adatintegritásra, a kölcsönös hitelesítésre, a hálózati biztonságra, a rugalmasságra és a hosszabb kulcsok alkalmazására. Ezeknek az együttes használata fokozott védelmet nyújt a hamis bázisállomás támadások ellen úgy, hogy a mobileszköz képes a hálózat azonosítására bizonyos jelzőüzenetek segítségével a hitelesség ellenőrzésére. A hamis bázisállomás támadás során a támadó egy bázisállomásnak álcázza magát, és képes lehet a titkosítási algoritmusok elnyomására vagy azok megváltoztatására. Amennyiben új fenyegetettségek jelennek meg a biztonsági funkciók igény szerint bővíthetők és javíthatók.

1.5 A 4. generációs mobilhálózatok

A 4G a mobilhálózati technológia következő generációja. Az ITU a 4G esetében is elkészítette a követelményrendszerét, melyre a szabványosító szervezetek támaszkodhatnak munkájuk során. Az ITU 2008-ban készítette el az IMT-Advanced ajánlást, ami a 4G rendszerekre vonatkozik, mely alapján a következő követelményeknek kell megfelelnie a mobilrendszereknek:

- teljesen IP-alapú csomagkapcsolt hálózatra kell épülnie;

- legyen képes a hálózati erőforrásokat dinamikusan megosztani és használni cellánként több felhasználó egyidejű támogatására;
- használjon skálázható csatornaszélességet 5-20 MHz-ig, opcionálisan 40 MHz-ig;
- magas mobilitás esetén legyen a maximális adatátviteli sebesség kb. 100 Mbit/s, alacsony mobilitás esetén 1 Gbit/s;
- legyen a kapcsolat spektrális hatékonysága 15 bit/s Hz lefelé irányuló kapcsolaton, 6,75 bit/s Hz felfelé irányuló kapcsolaton;
- legyen a rendszer spektrális hatékonysága beltéri helyeken 3 bit/s Hz lefelé, 2,25 bit/s Hz felfelé irányuló kapcsolat esetén.

Ezeknek a követelményeknek a 3GPP által szabványosított LTE (Long Term Evolution), a későbbi LTE Advanced és az IEEE által megalakított 802.16m vagy WiMAX szabványok feleltek meg, azonban kezdetben ezek a rendszerek sem garantálták az 1 Gbit/s-os adatátviteli sebességet.

Az LTE egy nagy sebességű technológia a mobil eszközök számára. A 3GPP a GSM/EDGE és az UMTS/HSPA technológiákra alapozva fejlesztette ki. A régebbi hálózatokhoz képest gyorsabb letöltési és feltöltési sebességet, alacsonyabb késleltetési időt és jobb lefedettséget kínál. Az LTE képes kihasználni a meglévő 2G és 3G, valamint az új spektrumokat. Magyarországon leginkább a 800, 1800 és 2600 MHz-s tartományokban működik, népsűrűségtől függően. Gyakran 4G hálózatokkal együtt említik, de csak 100 Mbit/s letöltési és 50 Mbit/s feltöltési sebességet képes elérni. Magyarországon az első 4G szolgáltatást a Magyar Telekom indította el 2012-ben.

Az LTE Advanced az LTE jelentős továbbfejlesztése, amit a 3GPP a Release 10-ben szabványosított. Az első LTE Advanced hálózat 2009-ben indult el Svédországban és Norvégiában, a következő évben pedig az USA-ban és Japánban lett kiépítve. Az LTE és az LTE Advanced között leginkább az adatátviteli sebességben van különbség, illetve az adótornyok és a készülékek közötti átvitel is jobban működik. Az adatot szűkebb frekvenciatartományban kezeli, amivel nagyobb kapacitást és stabilabb kapcsolatot biztosít. Technológiai újdonságnak tekinthető az úgynevezett vivőaggregáció. Ennek az a lényege, hogy a magasabb adatátviteli sebességhez, több frekvenciablokkot fognak össze egy egésszé, amit egy felhasználóhoz rendelnek. Így nemcsak az átviteli sebesség nő meg, hanem a rendszer erőforrás kihasználtsága is jobb lesz. Meg kell említeni a MIMO (Multiple Input and Multiple

Output) technológiát is. A technológia megsokszorozza a kapacitást kétszer annyi antenna használatával, az energiafogyasztás emelése nélkül. [6]

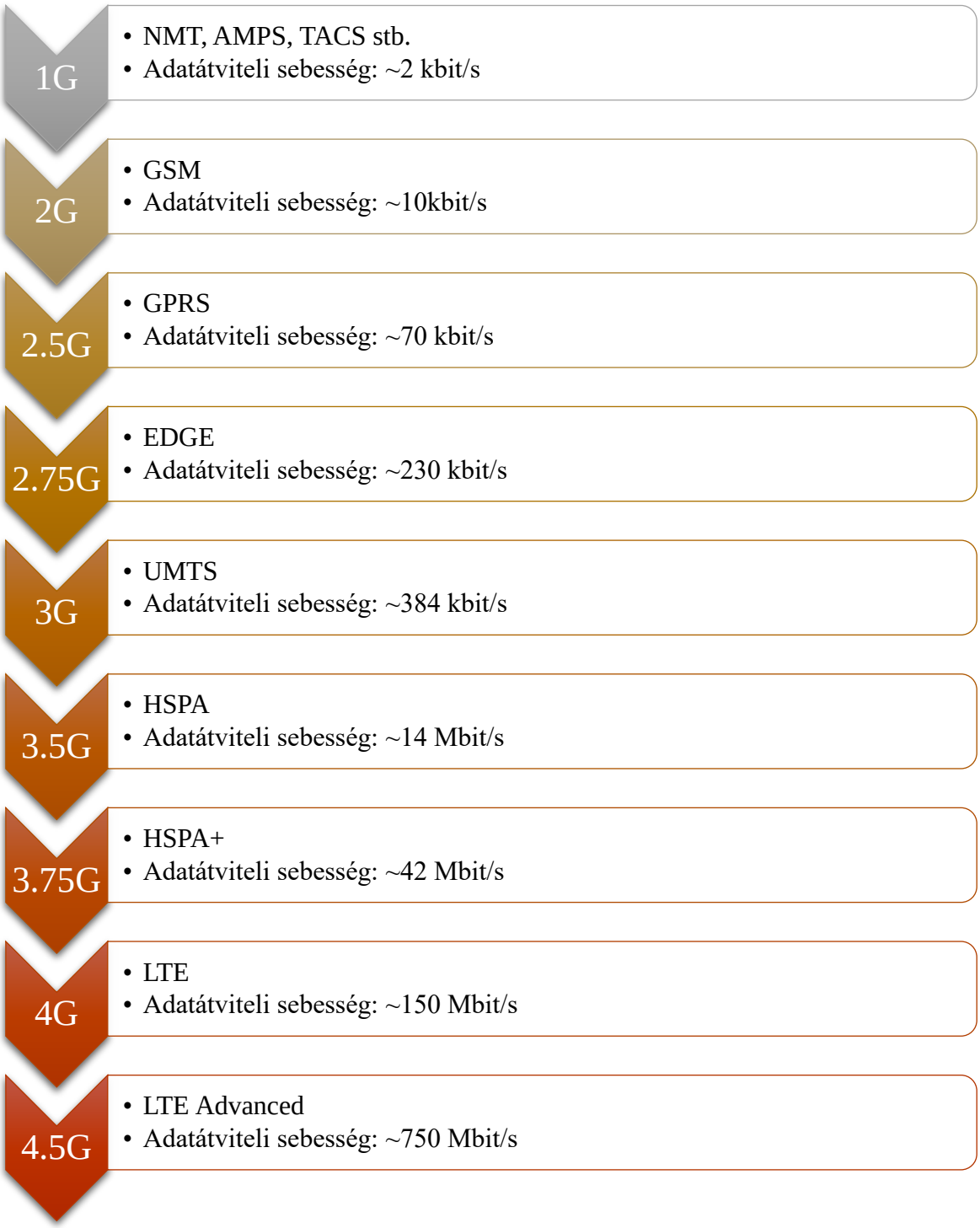
Az LTE biztonsági architektúráját a 3GPP határozta meg. Biztonsági rések lehetnek a SIM kártyák, az UICC[3] (Universal Integrated Circuit Card) tokenek, az eszköz és hálózat azonosítása, az éteren keresztüli védelem és hálózatvédelem esetében. Ezeknek a biztonsági réseknek a védelme történhet különböző titkosítási algoritmusokkal vagy a fizikai biztonság megfelelő kialakításával. Az LTE-től elvárt, hogy garantálja a bizalmas működést és az erős hitelesítést. Az LTE hálózatok azonban sebezhetők olyan biztonsági fenyegetésekkel szemben, amelyek megzavarják a rendelkezésre állást és a hitelesítést. Egyetemi kutatók egy alacsony költségvetésű, nyílt forráskódú szoftverrel további biztonsági réseket tártak fel a 4G hálózatokban. Eredményeik közül kiemelendő a hitelesítéses támadás, amely lehetővé teszi a támadó számára, hogy csatlakozzon a maghálózathoz, miközben az áldozat mobileszközének adja ki magát. Ennek során a támadó meg tudja határozni az áldozat helyét a hálózatban, és nemcsak a helyinformációkat tudja saját céljaira használni, hanem szolgáltatásmegtagadási támadásokat is indíthat. Ezzel a szolgáltatásmegtagadási támadással elérheti, hogy az áldozat készüléke ne kapjon értesítéseket (pl.: hívás, SMS), de azt is megteheti, hogy kitalált üzeneteket küld, amivel energia kimerülést okoz.

1.6 Összefoglalás

A mobilkommunikáció területén a "generáció" általában a szolgáltatás alapvető jellegének megváltozását, magasabb adatátviteli sebességet, új frekvenciasávokat, szélesebb frekvenciasávot jelent, melynek eredménye a kapacitás növekedése, azaz több felhasználó kiszolgálására alkalmas. A jobb minőségi paraméterek a szolgáltatások minőségi javulásához, a hívások érthetőségének növekedéséhez vezetnek, illetve a biztonsági követelményeknek a kielégítése is könnyebben végrehajtható feladat új biztonsági kockázat megjelenése esetén is.

A mobil szabványok új generációja körülbelül minden tízedik évben jelenik meg az 1G rendszerek 1970-es évek végi és 1980-as évek eleji bevezetése óta. Az 1G analóg átviteléről a 2G digitális átvitelére az átállás 1990-es évek elején ment végbe. Ezt követte a 2000-es évek elején a 3G multimédiás támogatás, majd 2010-es évek elején a 4G IP alapú hálózata.

[3] A SIM-hez hasonló intelligens kártya, amely több alkalmazással és nagyobb biztonsággal rendelkezik.



1. ábra A mobilhálózatok generációnak fejlődése az adatátviteli sebesség tükrében

Forrás: a szerző saját szerkesztése

A 4G és az 5G technológiák térhódításával csökken a régebbi technológiákat alkalmazó eszközök száma. A szolgáltatóknak el kell dönteniük, hogy meddig üzemeltetik a 3G hálózataikat. A régebbi hálózatok lekapcsolása mellett környezetvédelmi, energiatakarékossági

szempontok is szólnak, a felszabaduló sávokat pedig az új mobiltechnológiák hatékonyabban használják ki. A 3G hálózatok lekapcsolása az elkövetkezendő 1-3 évben várható.

2. AZ 5G JELLEMZŐI ÉS SAJÁTOSSÁGAI

Az 5. generációs mobilhálózat egy újfajta hálózatot tesz lehetővé, amely gyakorlatilag mindenkit és mindent összekapcsol, beleértve a gépeket, tárgyakat és az eszközöket is. Az 5G vezeték nélküli technológia célja, hogy még nagyobb adatátviteli sebességet, rendkívül alacsony késleltetést, még nagyobb megbízhatóságot, hatalmas hálózati kapacitást, még nagyobb rendelkezésre állást és egységesebb felhasználói élményt biztosítson több felhasználó számára a korábbi generációk nyújtotta technológiai lehetőségekhez képest. A nagyobb teljesítmény és hatékonyság új felhasználói élményeket biztosít, és új iparágakat köt össze.

Az 5G az űrkutatásnak köszönheti létezését. A NASA olyan vezeték nélküli hálózat kifejlesztésébe kezdett 2008-ban az M2MI nevű céggel együtt, amely apró műholdak rendszerbe szervezése céljából képes kis energiafelhasználás mellett, nagyon rövid idő alatt, nagy mennyiségű adat továbbítására. 2019-re a technológia rendelkezésre állt már a távközlési cégek számára is. Európában és Magyarországon 2020 júniusára váltak elérhetővé az 5G-s szolgáltatások. Olyan új szolgáltatások, alkalmazások jelentek meg, amelyeket korábban még nem ismertünk.

Az 5G szabványosításával „jelenleg főleg nemzetközi szabványosító szervezetek, elsősorban a 3GPP és az ITU, újabban az ETSI, illetve egyéb az informatikával, telekommunikációval, az információ átvitellel foglalkozó szervezetek foglalkoznak”. [7] Az ITU az 5G hálózatokra, eszközökre és szolgáltatásokra vonatkozóan is elkészítette a követelmény rendszerét, amit 2015-ben adott ki, és IMT-2020 néven lett ismert. Ennek célja az volt, hogy megfelelő 5G technológiákat fejlesszenek ki. Az IMT-2020 első kiadása magában foglalja a rádió-hozzáférési technológiák részletes műszaki előírásait, melyek a következők:

- legyen a csatlakozási sűrűség minimális követelménye 1 millió eszköz négyzetkilométerenként;
- legyen a lefelé irányuló csúcs adatátviteli sebesség 20 Gbit/s, a felfelé irányuló csúcs adatátviteli sebesség 10 Gbit/s;
- legyen a felhasználó által tapasztalt lefelé irányuló adatátviteli sebesség az idő 95%-ban sűrű városi környezetben tesztelt adatátvitel esetén 100 Mbit/s, a felfelé irányuló adatátviteli sebesség pedig 50 Mbit/s;

- legyen a mobilitás maximális sebessége az átadás- és a szolgáltatásminőség-követelményekhez 500 km/h;
- legyen a késleltetés 4 ms;
- legyen a csatlakozási sűrűség minimális követelménye 1 millió eszköz négyzetkilométerenként
- legyen az energiahatékonyság az elküldött vagy a fogadott adatok esetén egyenlő a 4G-nél meghatározottakkal;
- legyen a területi forgalom kapacitása 10 Mbit/s négyzetméterenként;
- legyen a csúcs lefelé irányuló spektrumhatékonyság, azaz az egységnyi vezeték nélküli sávszélesség és hálózati cellánkénti áteresztőképesség 30 bit/s/Hz.

Ezeknek a követelményeknek nem célja, hogy korlátozzák képességben és teljesítményben az IMT-2020-ra jelölt technológiákat, továbbá az sem, hogy meghatározzák, hogy hogyan teljesítsenek ezek a technológiák tényleges telepítésekben.

Az előbbi követelményekre támaszkodva a globális „mobilkommunikációs technológiák hálózatfejlesztési szabványosításának szinte teljes mértékben, az alkalmazásfejlesztési szabványosításának pedig jelentős részben a 3GPP a vezető testülete. Az általuk kidolgozott szabvány-jellegű dokumentumok kezdetben még nem foglalták magukban a teljes, mindenre kiterjedő 5G-s technológia képességeit”. [7] Ezt majd több, egymást követő, már elkészült, vagy jövőben elkészülő dokumentum fogja tartalmazni.

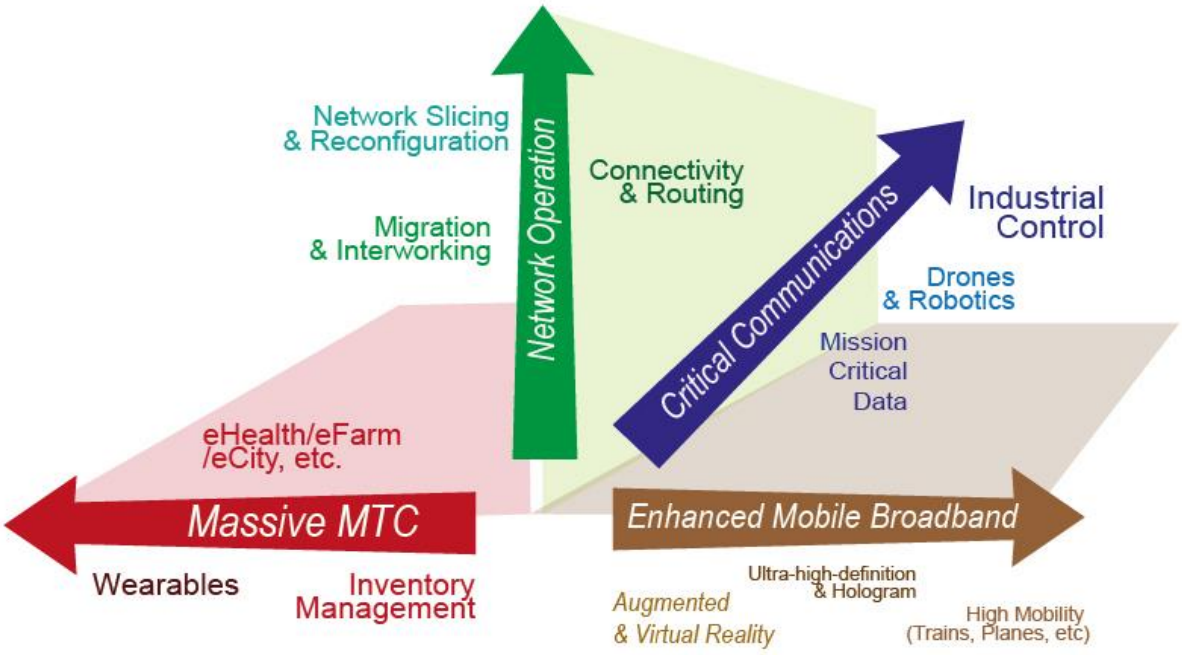
Ahogy azt korábban említettem, amikor a mobilhálózati generációk elértek egy döntő pontig a fejlődésük során, akkor a 3GPP mindig egy új kiadást készített. A kiadást nevezhetjük „Release”-nek is, ami már egy megvalósítható állapotot jelent az adott generációban. Az 5G-hez a Release 14, 15, 16, 17 és 18 kapcsolódik. Mivel az 5G bevezetése új lehetőségeket rejt magában, ezért lett több kiadásban specifikálva.

2.1 Release 14

A 3GPP a Release 14-ben új eseteket határozott meg az 5G számára, a SMARTER (Study on New Services and Markets Technology Enablers) projekt részeként. A projekt fő célja az új és továbbfejlesztett szolgáltatások, jellemzők és képességek mérlegelése és tanulmányozása, valamint a megfelelő követelmények meghatározása, különös tekintettel a következőkre: az új 5G hozzáféréssel kapcsolatos szolgáltatások támogatása, a kritikus szolgáltatási szempontok, a szabályozási szempontok és a vertikális piacok támogatása. Ezeket úgy érik el, hogy magas szintű használati eseteket alkalmaznak, és meghatározzák, hogy az 5G-

nek milyen funkciókat és funkcionalitást kell biztosítania. A kutatás 2015-ben indult el, amely több mint 70 felhasználási esetet tartalmaz. Az eseteket a következő nagyobb csoportokra kategorizálja:

- Enhanced Mobile Broadband (például: mobil szélessáv, mobilitás stb.);
- Critical Communications (például: ipari vezérlés, interaktív játék, drón irányítás stb.);
- Massive Machine Type Communications (például: hordozható eszközök, eHealth stb.);
- Network Operations (például: hálózat szeletelés, útválasztás, energiatakarékosság stb.);
- Enhancement of Vehicle to Everything (például: önvezetés stb.)



2. ábra A felhasználói esetek csoportjai [8]

Az Enhanced Mobile Broadband vagy a továbbfejlesztett mobil szélessáv (a továbbiakban: eMBB) a meglévő 4G szolgáltatások kiterjesztése, ami az első 5G szolgáltatások egyike, amely gyorsabb adatátviteli sebességet és ezáltal jobb felhasználói élményt biztosít, mint az előző mobil szélessávú szolgáltatások. Az eMBB számos különböző használati esetcsaládot tartalmaz, amelyek nagyobb adatsebességgel, nagyobb sűrűséggel, telepítéssel és lefedettséggel, nagyobb felhasználói mobilitással, rendkívül változó felhasználói adatsebességgel rendelkező eszközökkel, vezetékes mobilkonvergenciával és kiscellás telepítésekkel kapcsolatosak. Az 5G-nek nagyobb kapacitást kell biztosítania sűrűn lakott területeken, bel- és kültéren egyaránt. Például városközpontokban, irodaházakban vagy nyilvános helyszíneken, például stadionokban vagy konferenciaközpontokban. Az 5G

továbbfejlesztett kapcsolódást kell, hogy használjon a folyamatos felhasználói élmény biztosítása érdekében, azaz mindenhol elérhetőnek kell lennie. Az 5G-nek támogatnia kell a magasabb felhasználói mobilitást mozgó járművekben, beleértve az autókat, buszokat, vonatokat és repülőket. A korábban leírt IMT-2020 pontok többsége az eMBB-re vonatkozik. Az eMBB az 5G kezdeti fázisának tekinthető.

A Critical Communications olyan felhasználói eseteket tartalmaz, ami a kritikus fontosságú kommunikációt érinti, azaz a késleltetést, a megbízhatóságot és a rendelkezésre állást. Ezeket a követelményeket továbbfejlesztett rádióinterfésszel, optimalizált architektúrával, valamint dedikált mag- és rádió erőforrásokkal lehet teljesíteni. A tanulmány célja olyan használati esetek kidolgozása, amik a kereskedelmi- és közbiztonságot érintik, valamint a lehetséges szolgáltatási és működési követelmények meghatározása, hogy a hálózatüzemeltetők támogatni tudják a kritikus kommunikációt. A következő használati esetcsaládokat azonosították a kritikus kommunikáció területén: nagyobb megbízhatóság, nagyon alacsony késleltetés, nagyobb pontosságú pozicionálás, magasabb rendelkezésre állás és Mission Critical Services (pl.: vészhelyzeti kommunikációs rendszerek, villamosenergia-hálózati rendszerek). Az UAV-k (Unmanned Aerial Vehicles) és a földi járművek távvezérlése jól illeszkedik a nagyobb megbízhatóság és alacsonyabb késleltetés közé, hiszen a mozgó eszközöket gyorsan és megbízhatóan kell irányítani. A késleltetésnek azonban nem kell rendkívül alacsonynak lennie, ha emberi kezelő is részt vesz, mert az emberi reakciósebesség határozza meg a késleltetés várható szintjét, és nincs értelme a kommunikációs hálózattól sokkal alacsonyabb késleltetést kérni, mint a kezelője által okozott. A számítógéppel vezérelt eszközök esetében a nagyon alacsony késleltetés lényeges követelmény lehet.

A Massive Machine Type Communication (a továbbiakban: mMTC) a nagyszámú eszközöket tartalmazó használati esetek csoportja, amelyek jellemzői és igényei széles skálán mozognak. Az intelligens szolgáltatások elterjednek a városi területeken, és a használat az elővárosi és vidéki területeken is növekedni fog. Mindezen szolgáltatások összevonása a nagyon eltérő tulajdonságokkal rendelkező eszközök nagyon nagy sűrűségéhez vezet, amelyeket várhatóan egy közös kommunikációs és együttműködési keretben egyesítenek. A tömegesség kihívása új vezeték nélküli technológiák kifejlesztését indította el. A fő cél olyan rendszerek fejlesztése, amelyek nagyszámú, nagy területen elosztott, alacsony költségű eszközt, valamint rendkívül alacsony fogyasztású és különféle típusú szolgáltatásokat támogatnak. Ez a használati esetcsoport különösen releváns az új vertikális szolgáltatások esetében, mint például az okos

otthon, az okos város, az intelligens segédprogramok, az e-Health és az okos hordozható eszközök.

A Network Operations feladata, hogy azonosítsa és rögzítse a kívánt rendszerkövetelményeket és képességeket a hálózatüzemeltetők számára az új lehetőségek kiépíthetőségéhez. A SMARTER tanulmányban ez a csoport kizárólag a hálózat működésével kapcsolatos. Az esetcsaládokból kiindulva meghatározza a hálózati működés követelményeit, melyek tartalmazzák a rendszer rugalmasságát, a skálázhatóságot, a mobilitás támogatását, a hatékony tartalomszolgáltatást, az ön-visszacsatolást, a hozzáférést, a migrációt, illetve a régi rendszerekkel való együttélést, az optimalizálást és a biztonságot. Ellentétben a korábbi rendszerekkel, az 5G képes egyidejűleg optimalizált támogatást nyújtani a különböző konfigurációkhoz különböző eszközökön keresztül. A hálózati funkcionalitás és a szolgáltatás rugalmassága és alkalmazkodóképessége az 5G rendszer kulcsfontosságú megkülönböztető jellemzője. A rugalmasság céljának eléréséhez az egyik kulcsfontosságú koncepció a hálózati szeletelés. A hálózatszeletelés lehetővé teszi az üzemeltető számára, hogy dedikált logikai hálózatokat biztosítson. A rugalmasságot tovább erősíti a hatékony felhasználói sík, a rugalmas broadcast szolgáltatás, a szolgáltatók közötti hálózati kapcsolat és szolgáltatás csere, valamint a szolgáltatás minősége.

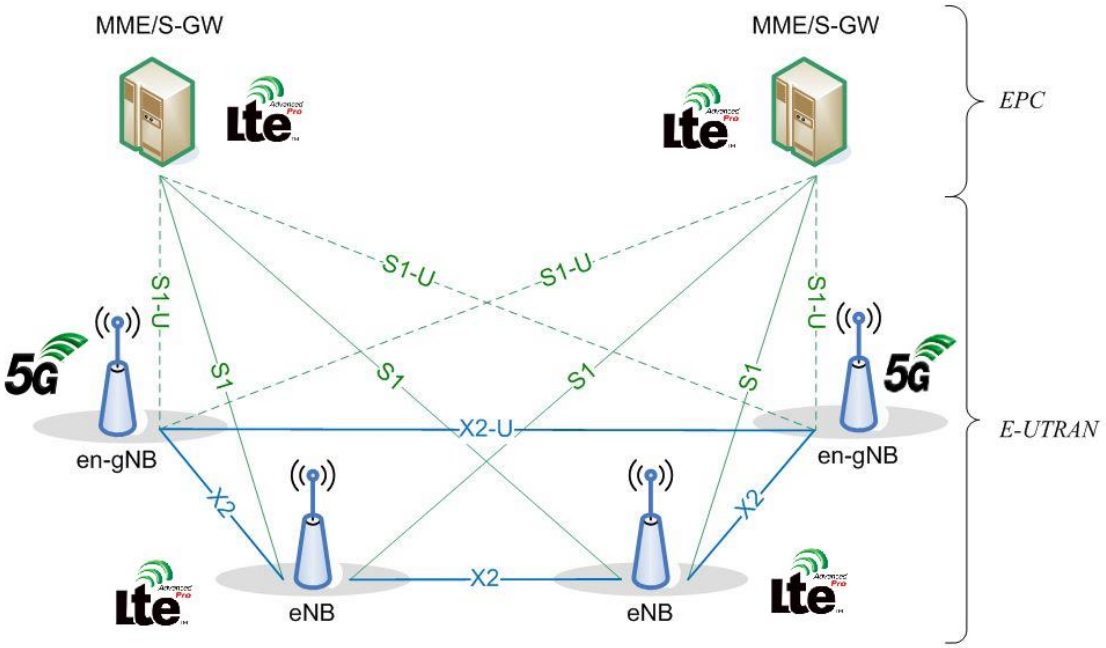
2.2 Release 15

Egy teljesen új szabvány meghatározása az 5G számára nagy vállalkozás. A 3GPP fő munkaterülete a Release 15-ben a mobilkommunikáció ötödik generációja kezdeti szakaszának meghatározása. A 3GPP az 5G szabványosítását két kiadásra osztotta. Az első fázist a Release 15, míg a második fázisát a Release 16 tartalmazza. A különféle felhasználói felületek, szolgáltatások és technológiák támogatásának igénye a technológiai forradalmat egy nagy teljesítményű és rendkívül hatékony rendszer felé terelte. Az előzők közé tartozik a dolgok internete, a virtuális valóság, az ipari vezérlés, a mindenütt jelen lévő igény szerinti lefedettség, valamint a testreszabott piaci igények kielégítésének lehetősége. Ezekhez jól bevált eszközök, szolgáltatások és technológiák fejlesztésére volt szükség a 3GPP által. Az 5G rendszer fő célja, hogy képes legyen támogatni az új telepítési forgatókönyveket a különböző piaci szegmensek kezelésére. Az 5G-t úgy tervezték, hogy támogassa a különféle szolgáltatásokat különböző adatforgalmi profilokkal (pl.: nagy áteresztőképességű, alacsony késleltetésű kapcsolatok) és modellekkel (pl.: IP adatforgalom, nem IP adatforgalom). A kiadás 2017-ben indult el, és 2019-ben fejeződött be. A Release 15 specifikációi leírják az új rendszerarchitektúrát és az 5G rendszerhez szükséges eljárásokat és meghatározó követelményeket.

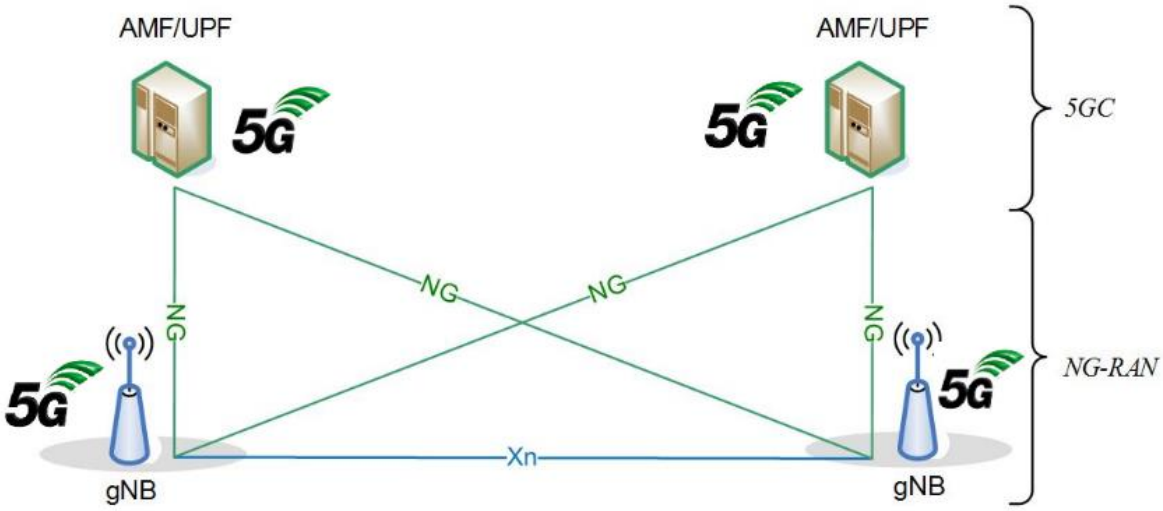
Az 5G rendszer első fázisa mellett a Release 15 többek között magában foglalja: a kritikus kommunikációt (beleértve az ultra megbízható alacsony késleltetésű kommunikációt, a továbbiakban: URLLC), az mMTC és az IoT további fejlesztéseit, a járművekkel kapcsolatos kommunikációt, a Mission Critical, valamint a WLAN-hoz és a licenc nélküli spektrumhoz kapcsolódó szolgáltatásokat.

Az 5G fő jellemzője egy új rádiós interfész, a New Radio (NR) bevezetése volt, amely biztosítja a szükséges rugalmasságot ezeknek a nagyon különböző típusú szolgáltatásoknak a támogatásához. Az 5G másik kulcsfontosságú jellemzője, hogy az 5G hozzáférési hálózat nem csak egy új 5G maghálózathoz, hanem a meglévő 4G (LTE) maghálózathoz is csatlakozhat. Ezt „Non-Stand Alone" (a továbbiakban: NSA) vagy nem önálló architektúrának hívják. Az NR teljes verziójának tényleges megvalósításához hatalmas mennyiségű új hardvert kell telepíteni. A másik 5G architektúrát „Stand Alone"(a továbbiakban: SA) vagy önálló architektúrának nevezik.

Az NSA architektúra az, ahol az 5G rádiós hozzáférési hálózat és annak új rádiós (NR) interfésze a meglévő LTE hálózattal együtt kerül felhasználásra, így hálózatcsere nélkül elérhetővé válik az NR technológia. Az NSA architektúra átmeneti lépésnek tekinthető a „teljes 5G" kiépítés felé, amelyben csak a 4G szolgáltatások támogatottak, de azok élvezik az 5G NR által kínált kapacitásokat (pl.: alacsonyabb késleltetés stb.), illetve kettős csatlakozást is kínál.

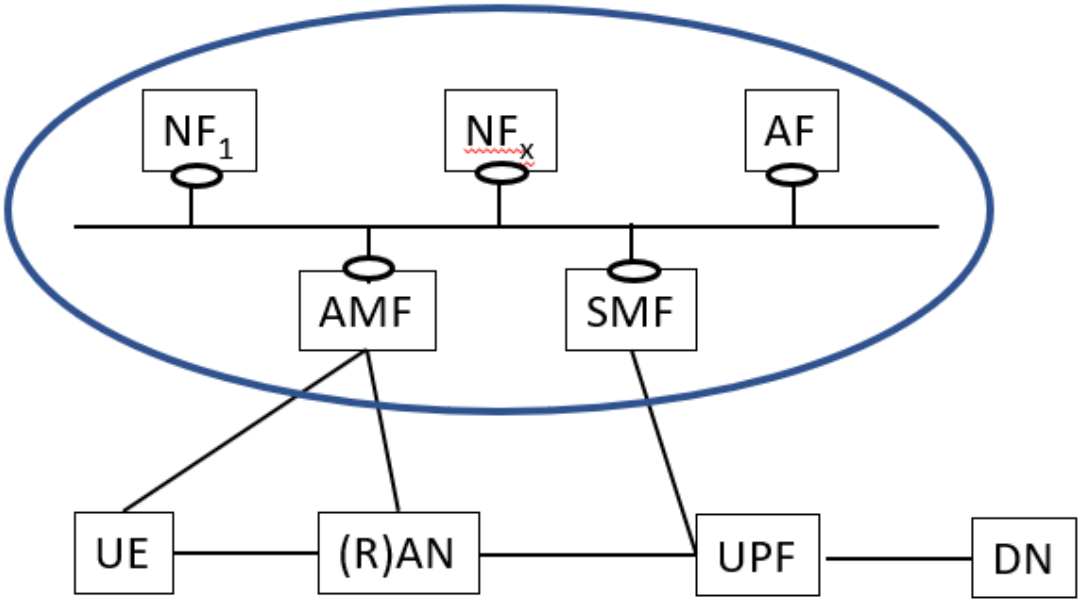


3. ábra NSA architektúra [9]



4. ábra SA architektúra [9]

Az SA architektúra az, ahol az NR az 5G saját maghálózatához kapcsolódik. Csak ebben a konfigurációban támogatott az 5G első fázisa szolgáltatásainak a teljes készlete. Az SA telepítési opcióban az 5G rendszer a felhasználói berendezésekből, a hozzáférési hálózatból (beleértve az NR-t) és a maghálózatból áll.



5. ábra Az 5G rendszer felépítése [9]

A kékkel bekarikázott területen a maghálózat található. A maghálózat nem hagyományos hálózati elemekből épül fel. Az elemeket hálózati funkció szerint határozzák meg, melynek előnye, hogy a közös rendszeren keresztül bármely másik hálózati funkció vagy felhasználó elérheti az adott szolgáltatást, vagyis virtualizálható. Az ilyen megközelítés modularitást és

újrafelhasználhatóságot kínál. A legfontosabb maghálózati funkciók közé tartozik a hozzáférés és mobilitás menedzsment funkció (a továbbiakban: AMF), a felhasználói sík funkció (a továbbiakban: UPF) és a munkamenet kezelés funkció (a továbbiakban: SMF). Ezek a funkciók információt cserélnek a maghálózat és a hozzáférési hálózat között. Az AMF különböző mobilitási igényekkel rendelkező felhasználói berendezéseket támogat, a feladatai a mobilitásra, a hozzáférésre és a biztonságra irányulnak. Az SMF gondoskodik a felhasználói adatforgalommal kapcsolatos feladatokról, mint a munkamenet létrehozásáról, az IP címek kiosztásáról stb. Az UPF a felhasználói adatok kezelésével foglalkozik. Az architektúra mélyére nyúlik a maghálózat által biztosított funkciók területén. További funkciók foglalkoznak a tárhelyek biztosításával, az adatkezeléssel, a hálózat szeletelésével, a hozzáféréssel, a szolgáltatás minőségének támogatásával és a hálózati képességek megismerésével.

A hozzáférési hálózat kialakítása rendkívül egyszerű, hiszen egyetlen elemből áll. A hozzáférési hálózat egy sor bázisállomásból (a továbbiakban: gNB) áll, amelyek az NG interfészen keresztül kapcsolódnak a maghálózathoz. A gNB egy másik gNB-hez csatlakoztatható az Xn interfészen keresztül vagy egy 4G-s bázisállomáshoz csatlakoztatható X2 interfészén keresztül. A hozzáférési hálózat oldalán a gNB látja el az összes főbb hozzáférési hálózattal kapcsolatos feladatot, például: rádiós erőforrás-kezelési funkciók végrehajtása, IP-fejléc tömörítése, az adatok titkosítása, illetve integritásuk védelme, mérési és jelentési konfiguráció a mobilitáshoz és ütemezéshez, stb.

Az 5G két frekvenciatartományt támogat: FR1 (a 7 GHz alatti) és FR2 (milliméteres hullámtartomány).

Név	Frekvenciatartomány
FR1	410 MHz – 7125 MHz
FR2	24250 MHz – 52600 MHz

1. táblázat Az 5G frekvenciatartományai

Forrás: a szerző saját szerkesztése

A különféle telepítések kezeléséhez az NR a vivőfrekvenciák széles skáláját és több csatorna sávszélességet támogat a két lehetséges tartományon belül. A szélesebb sávszélesség elérése érdekében a vivő aggregáció legfeljebb 16 NR vivőt támogat. Az NR-t úgy tervezték, hogy támogassa az együttélést az LTE-vel, mivel az egyes NR frekvenciasávokat LTE-vivőkhöz használják. Az NR rugalmas alvivő-távolságot használ, amely az LTE-ben használt 15 KHz-es alapvivő-távolságból származik. Az NR az LTE-hez hasonlóan a ciklikus előtagú OFDM-et (a

továbbiakban: CP-OFDM) használja lefelé és felfelé irányuló kapcsolati hullámformaként. Az alábbi táblázat összefoglalja ezeket a jellemzőket a két frekvenciatartományra lebontva.

Jellemzők	FR1	FR2
Vivőaggregáció	legfeljebb 16 vívő	
Sávszélesség csatornánként	5,10,15,20,25,40,50,60,80,100 MHz	50,100,200,400 MHz
Alvivő-távolság	15,30,60 KHz	60,120,240 KHz
Hozzáférési séma	DL: CP-OFDM, UL: CP-OFDM	

2. táblázat Az 5G egyéb jellemzői

Forrás: a szerző saját szerkesztése

A Multiple Input, Multiple Output (a továbbiakban: MIMO) működése az NR kulcsfontosságú összetevője. Az 5G támogatja a nagyméretű antennatömböket, amelyeket gyakran „masszív MIMO-nak" nevezünk. Az NR teljes kialakítása sugár alapú, ami azt jelenti, hogy az összes nyaláb formázható a lefedettség, átviteli sebesség és a kapacitás növelése érdekében. Több antennát használ mind az adó, mind a vevő oldalon, hogy lehetővé tegye a többrétegű adatátvitelt. Az NR támogatja a többrétegű adatátvitelt egyetlen felhasználói eszköz és több felhasználói eszköz számára. Mivel az NR támogatja a többnyalábú működést, ahol minden jel és csatorna iránynyalábban kerül továbbításra, a sugárformálás fontos technika a nagyobb áteresztőképesség és a megfelelő lefedettség eléréséhez, különösen a magas frekvenciatartományban.

Az ultra-megbízható alacsony késleltetésű kommunikációt és a tömeges géptípusú kommunikációt is tartalmazza a Release 15. Az URLLC és az mMTC kifejezetten az eszközök és dolgok közötti kommunikáció megkönnyítésére szolgál (IoT), nem pedig az emberek közötti kommunikáció megkönnyítésére. A két kommunikációs típus létfontosságú az IoT fejlődő világában, és kulcsfontosságú az automatizálás jövője szempontjából. Az URLCC és az mMTC továbbfejlesztése elsősorban a felhasználói eszközök energiafogyasztásának csökkentésére, az air-interface és a protokollréteg egyes részeire koncentrál, mint például: a korai adatátvitel, nyugodt monitorozás a cella újraválasztásához, keskeny sávú mérési pontosság javítása, kis cellás támogatás, csökkentett rendszerszerzési idő stb.

2.3 Release 16

A Release 16 célja a szilárd Release 15 technológiai alap továbbfejlesztése az 5G rendszer teljesítményének és hatékonyságának javítása érdekében azért, hogy kulcsfontosságú

technológiákat kínáljon az új iparágak átalakításához. Ebben a tekintetben az 5G sokoldalúsága és megbízhatósága tovább nőtt, hogy az iparági szintű kompatibilitást elérje az URLLC, a hálózati szeletelés, az IoT, a nem nyilvános hálózatok és helymeghatározási szolgáltatások továbbfejlesztésével. Mindezen ipari szempontok mellett a Release 16 további fejlesztései kiterjednek az 5G és a nem 3GPP rendszerekkel való együttélésére, a szórakoztatásra, a hálózat optimalizálására, a licenc nélküli spektrum hozzáférésére, valamint néhány fejlesztés a mobilitást és az felhasználói eszközök energiatakarékosságát vizsgálja.

Az új vertikális felhasználási esetek, például a gyári automatizálás megoldása érdekében a Release 16 továbbfejleszti az 5G URLLC alapot, hogy még jobb linkmegbízhatóságot biztosítson (akár 99,9999%). Ezekben a felhasználási esetekben nem elegendő az újraküldések számának egyszerű növelése, hanem szükséges a redundáns kommunikációs útvonalak bevezetése, így ha egy útvonal átmenetileg blokkolva van, a kommunikáció megszakítás nélkül megtörténik a fennmaradó utak használatával. Különböző rétegekben különböző beállítások vannak a redundáns kapcsolatok támogatására. A redundáns átvitel támogatásán felül a QoS figyelés, a csomagkésleltetési költségvetés dinamikus felosztása és a munkamenet-folytonossági mechanizmus is része a továbbfejlesztett URLLC-nek, amelyek tovább növelik az 5G rendszer megbízhatóságát és csökkentik késleltetését. Az URLLC fejlesztések nemcsak a maghálózatot érintik, hanem a fizikai réteget is. A kiadás olyan fejlesztéseket határoz meg, amelyekkel jobb spektrum kihasználtságot és jobb figyelési képességeket érnek el. Az URLLC fejlesztésének fontossága, abból is látszik, hogy több réteget is érint az 5G felépítésében. Ezenfelül, hogy jobban támogassa a különféle vertikális piacok felhasználási eseteit, és hogy extra megbízhatóságot érjen el az URLLC, az NR tartalmaz csomagduplikációs, ütemezési, időzítési, tömörítési fejlesztéseket is.

Az 5G elérhetőségének a hagyományos nyilvános mobilhálózatokon túlmutató kiterjesztése érdekében a 3GPP a Release 16-ban három olyan projektet hajtott végre, amelyek elengedhetetlenek az új vertikális telepítésekhez.

Az első a licenc nélküli spektrum (a továbbiakban: NR-U) az 5 GHz-s sávban. Az NR-U kettő működési módot határoz meg. A horgonyzó NR-U során a licenc nélküli spektrum más licencelt vagy nem licencelt spektrumokkal van kombinálva, mint például az 5GHz-es sáv, amelyet a Wi-Fi széles körben használ. Az önálló NR-U esetében csak licenc nélküli spektrumot használnak. A megosztott és engedély nélküli spektrumhoz való hozzáférés több dimenzióban is kiterjeszti az 5G-t, például nagyobb kapacitást, magasabb spektrumkihasználást és új

telepítési forgatókönyveket tesz lehetővé. Előnyös lesz a licenccelt spektrummal rendelkező mobilszolgáltatóknak, ugyanakkor lehetőséget teremt a licenccel nem rendelkezők számára, hogy kihasználják az 5G technológiák előnyeit.

A második Release 16 projekt a nem nyilvános hálózatok támogatása. A magánhálózatok dedikált erőforrásokat használnak, amelyeket függetlenül kezelnek, és olyan biztonságot és adatvédelmet biztosítanak, amely lehetővé teszi, hogy az érzékeny adatok a helyszínen maradjanak, és optimalizálják a helyi alkalmazásokat. A magánhálózatok számos új 5G-előnyöket jelenthetnek az ipari IoT számára.

A harmadik projekt az időérzékeny hálózat integrációjának bevezetése. Ez egy determinisztikus kommunikációs szolgáltatás. A funkció megjelenik a szolgáltatásminőség és forgalmi jellemzőkben is, mint korlátozott késleltetés, megbízhatóság, átviteli csomópontok szigorú szinkronizálása stb.

A pozicionálási funkció nagy pontossága egyre fontosabbá válik az 5G-t használó ágazatok számára. A korábbi mobilhálózatok műholdas rendszeren alapuló helymeghatározást használtak, ami jellemzően a kültéri területekre korlátozódott. Az NR helymeghatározása során a helymeghatározó szerver összegyűjti, és szétosztja a helymeghatározással kapcsolatos információkat. A különböző esetekre (pl.: segélyhívások, ipari, logisztikai, e-health, légi esetek) vonatkozó pontossági követelmények teljesítése érdekében számos pozícionálási módszert alkalmaznak, mint a DL alapú, az UL alapú, vagy ezek együttes alkalmazása. A hangsúly többek között a pontosság javításán és a zökkenőmentes helymeghatározáson van a teljes 5G lefedettségben. A kiadás kiterjed a helymeghatározó funkció energiahatékonyságára is, amely számos felhasználási esetben kulcsfontosságú, mint például az eszközkövetés.

Az 5G NR hálózati lefedettség széles körű kiterjesztésének egyik kulcsfontosságú kihívása a további bázisállomások telepítésének költsége, amely általában új száloptikai backhaul[4] telepítéseket tesz szükségessé. A bázisállomások költséghatékonyabbá tétele érdekében a Release 16 integrált hozzáférést és backhaul-t (a továbbiakban: IAB) vezetett be, amely lehetővé teszi a bázisállomás számára, hogy vezeték nélküli hozzáférést biztosítson az eszközökhöz és vezeték nélküli backhaul kapcsolatot is, ezáltal nincs szükség vezetékes backhaulra. Az integrált hozzáférés egy rugalmasabb tömörítési stratégiának nyit ajtót, lehetővé

[4] A backhaul egy távoli helyről vagy hálózatról egy másik, általában egy központi helyre történő jel továbbítására utal. A backhaul rendszerint nagy kapacitású vonalat jelent, vagyis nagy sebességű vonalakat, amelyek nagy sávszélességet képesek nagyon gyors sebességgel továbbítani.

téve a kezelők számára, hogy gyorsan, dinamikusan adhassanak hozzá új bázisállomásokat, mielőtt további szálakat kellene beépíteniük a backhaul kapacitás növelése érdekében.

A Release 16 a MIMO teljesítményének és hatékonyságának további javítására is koncentrál. A Release 15 hiányosnak bizonyult a spektrális hatékonyság, a lefelé és felfelé irányuló kapcsolati átviteli teljesítmény, a jelzési késleltetés és a jelzési többletterhelés tekintetében. A kiadás számos technikai területen dolgozott ezzel kapcsolatban, beleértve a több felhasználós MIMO fejlesztését a magasabb rangok támogatása érdekében, a több átviteli és vételi pont támogatását, valamint a többnyalábú műveletek támogatását a kapcsolat megbízhatóságának javítása érdekében.

Az előbb említett területek csak egy részét képezik a Release 16 projekt széles körének. Sok más, alapvető 5G rendszer területet is tovább erősít a kiadás, beleértve a mobilitás kezelést, az energiatakarékosságot, az interferenciakezelést stb.

2.4 Release 17

A Release 17 számos funkciója a meglévő szolgáltatások és használati esetek (pl.: mobil szélessáv, ipari automatizálás stb.) hálózati teljesítményének javítását szolgálja, míg mások új használati esetekkel és telepítési lehetőségekkel (pl: közbiztonság, nem földi hálózatok, stb.) foglalkoznak. Az 5G kulcsfontosságú szempontja az új ágazatok és telepítési forgatókönyvek folyamatos támogatása. A Release 17 megerősíti az 5G támogatást az új felhasználási esetekben.

A Release 17 MIMO fejlesztések négy területet érintenek: nyalábkezelés; többszörös átviteli és vételi pont (a továbbiakban: mTRP) az URLLC részére, mTRP az eMBB-hez, valamint a TDD[5] (Time Division Duplex) és FDD[6] (Frequency Division Duplex) viszonosság. A többnyalábú fejlesztések célja, hogy javítsák a teljesítményt nagy mobilitás mellett a jelzések áramvonalasításával, és optimalizálják a felhasználói berendezések teljesítményét a valós telepítésekből tapasztalt problémákból. Az mTRP fejlesztések növelik a lefelé és felfelé irányuló kapcsolati vezérlőcsatornák robosztusságát. A kölcsönösség-alapú működés továbbfejlesztése közé tartozik az új kódkönyvek használata csökkentett többletterheléssel. A MIMO fejlesztések különösen fontosak az URLLC szolgáltatások megbízhatóságának

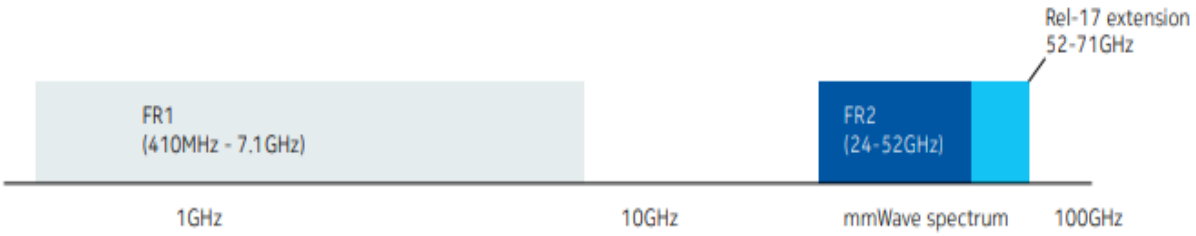
[5] Idő alapú spektrumhasználati technika.
[6] Frekvencia alapú spektrumhasználati technika.

biztosítása szempontjából és a több antennapanellel rendelkező eszközök mmWave frekvencián történő működésének támogatása szempontjából.

A Release 17 az 5G-ben először vezeti be a multicast kommunikáció támogatását elsősorban a kritikus kommunikáció, közbiztonság, vehicle-to-everything és vasutak számára. Az 5G multicast és broadcast szolgáltatás elsősorban a közbiztonság szempontjából fontos felhasználási esetek támogatására szolgál, mint például csoportos hívás, az éteren keresztüli szoftverfrissítések, élő tévéadás, videó továbbítás stb. A Release 17 ezenkívül lehetővé teszi a csoportos küldési munkameneteket a kapcsolt állapotban lévő eszközök számára, valamint a szórási munkameneteket a kapcsolt, inaktív és tétlen állapotban lévő felhasználói eszközök számára.

A Release 17 a nem földi hálózatokkal (a továbbiakban: NTN) új topológiákat vezet be a specifikációkba. Ezek a topológiák nagy magasságú platformokon és alacsony Föld körüli pályán, illetve geoszinkron pályás műholdakon alapulnak. Az NTN kiegészíti a földfelszíni hálózatokat hálózati lefedettséggel a tengeren és a szárazföldön túli távoli területeken, továbbá kiegészíti a szolgáltatásokat ott, ahol nincs földi lefedettség.

A Release 15-ben és 16-ban az 5G NR-t úgy tervezték, hogy FR1 és FR2 frekvenciatartományokban is működjön. A Release 17 egyik fő lépése ezen a területen az NR támogatásának bevezetése az 52–71 GHz-es frekvencián, amit az alábbi ábra mutat.



6. ábra A frekvenciatartomány kiterjesztése [10]

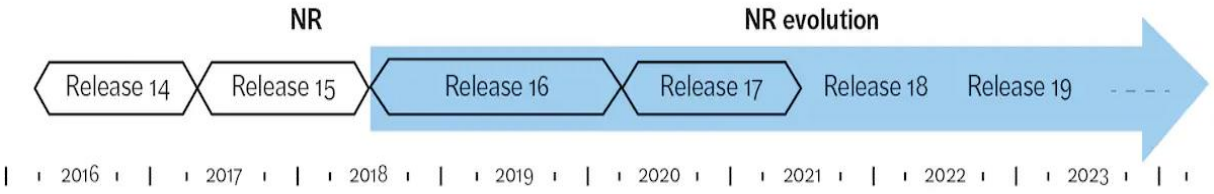
Az NR 52,6 GHz-nél magasabb frekvencián történő működtetése nagy kapacitást biztosít a szolgáltatók számára olyan speciális felhasználási esetekben, mint például a mobil szélessávú szolgáltatások beltéri és sűrű városi esetekben. A Release 17-ben a frekvenciatartomány az 52,6 GHz-en túl egészen 71 GHz-ig van kiterjesztve, és magába foglal új engedélyezett és nem engedélyezett frekvenciasávokat is.

A Release 16-ban a 3GPP a nem nyilvános hálózatok támogatását írta elő, amelyek hozzáférést biztosítanak a felhasználók egy bizonyos csoportjára, például az adott gyárhoz tartozó eszközökre. Az ipari vertikumok teljes körű támogatása érdekében a 3GPP két NPN telepítési lehetőség támogatását írta elő. Az első lehetőség nyilvános hálózatba integrált NPN. A második telepítési lehetőség önálló NPN (a továbbiakban: SNPN) néven ismert. A 3GPP további fejlesztéseket biztosít a Release 17 SNPN-jeihez. Ezek a fejlesztések magukban foglalják az SNPN-hez külső hitelesítő adatokkal való hozzáférést és a felhasználói eszköz beépítését az SNPN-be.

Az URLLC kulcsfontosságú tényezője az 5G rendszernek. A Release15 szilárd alapot teremtett, a Release 16 pedig további fejlesztéseket vezetett be, hogy jobban kiszolgálja a különféle iparági területeket. A Release 17 fejlesztéseinek célja a spektrális hatékonyság és a rendszerkapacitás javítása, az URLLC támogatása nem engedélyezett spektrumkörnyezetekben, valamint az időérzékeny kommunikáció megerősítése.

2.5 Összefoglalás

A 3GPP 2018-ban tette közzé az 5G szabvány első verzióit. A specifikációk három fő területre oszlanak: rendszer architektúra, maghálózat, valamint a hozzáférési hálózat. Az 5G hozzáférési hálózat NR (New Radio) néven is ismert. A 3GPP folyamatos számozási sémával kiadásokba szervezi a munkáját. Az 5G specifikációk első verziója 2018-ban jelent meg a Release 15-ben, amely az alapfunkciókat biztosította.



7. ábra A kiadások időpontjai [11]

Ahogy az előző ábrán látszik a következő kiadásokban a 3GPP új funkciókkal egészítette ki a meglévő alapvonalat. Ez visszafelé kompatibilis, így a régebbi terminálok továbbra is működhetnek frissített hálózatokban és fordítva. A 3GPP olyan funkciókat ad hozzá, amelyek a meglévő szolgáltatásokkal szembeni növekvő igények vagy az új szolgáltatások, használati esetek és telepítési lehetőségek követelményeinek kielégítéséhez szükségesek.

A 3GPP Release 16 nemcsak a szilárd Release 15 technológiai alapot fejleszti tovább az 5G rendszer teljesítményének a lefedettség, a kapacitás, a késleltetés, az energia, a mobilitás, a megbízhatóság stb. szempontjainak javítása érdekében, hanem ezenfelül kulcsfontosságú technológiákat is kínál az új iparágak átalakításához.

A 3GPP 17. kiadása a korábbi kiadásokra épít azzal a céllal, hogy javítsa az 5G rendszer teljesítményét, támogassa az új felhasználási eseteket és vertikumokat, valamint mindenütt elérhető kapcsolatot biztosítson a különböző telepítési feltételek és forgatókönyvek esetén.

A következő fázisban a 18-as kiadás létrehozza az 5G Advanced-et, amely új megoldásokat és technológiai összetevőket tartalmaz majd, melyek továbbra is növelik a mobil szélessáv és a vertikális hálózatok teljesítményét. Az 5G Advanced a vezeték nélküli hálózatokba is több intelligenciát vezet be azáltal, hogy megfelelő gépi tanuláson alapuló technikákat épít be a hálózat különböző szintjein. Az 5G-hez hasonlóan az 5G Advanced is képes lesz az összes használati esetet egyetlen rendszertervezésből támogatni a továbbítási kompatibilitásra és a változatos konfigurálhatóságra összpontosítva, miközben a lehető legnagyobb egyszerűséget biztosítja.

3. AZ 5G BIZTONSÁGI KÉRDÉSEI ÉS KOCKÁZATAI

A vezeték nélküli kommunikáció célja egy megbízható és kiváló minőségű kommunikáció biztosítása. Az 5G egy előrelépés ebben az irányban, hiszen megváltoztatta az emberek és az eszközök kapcsolódási módját, gyorsabb adatsebességet, alacsony késleltetést, nagyobb megbízhatóságot, nagyobb hálózati kapacitást, jobb rendelkezésre állást és jobb felhasználói élményt biztosítva. Mint minden új technológia esetében, az 5G bevezetése is új biztonsági kihívásokat eredményezett.

A korábbi generációkban a biztonság kialakítása összességében sikeresnek mondható, hiszen csak néhány alapvető szolgáltatást (pl.: hang és adatvédelem) kell védeni. Mivel korlátozottak a támadási lehetőségek, ezért azok célzott védelmi tevékenységekkel elháríthatók. A felhasználói oldal részéről ilyen tevékenység az adattitkosítás, az alapvető identitásvédelem, a hálózati oldalon pedig az erős hitelesítés. Az idő múlásával azonban új fenyegetések jelentek meg, amit az új generációkba beépített ellentevékenységgel kezeltek.

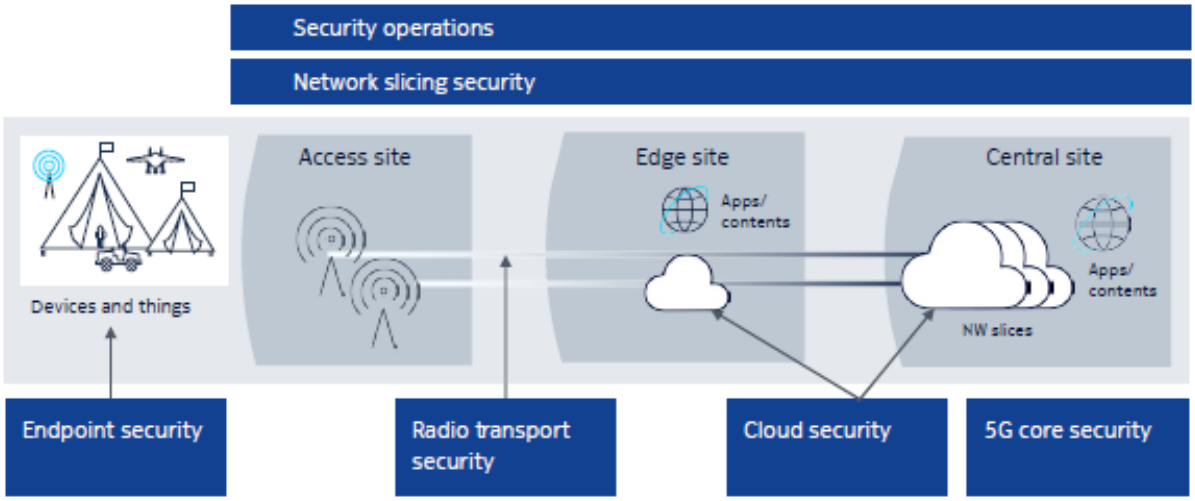
A fenyegetések és a technológiák fejlődésével az 5G új megközelítéseket igényel a biztonság terén. Az 5G-ben egyre több szereplő vesz részt a szolgáltatásnyújtásban, akik akár dinamikusabban is kezelhetik a hálózataikat virtualizált hálózati funkciót használva, amelyek

több, különböző biztonsági tapasztalatokkal és hozzáállással rendelkező beszállítóktól származnak.

A biztonság új megközelítése megköveteli, hogy a szolgáltatók kulcsfontosságú képességeket alkalmazzanak. Az egyik ilyen képesség az alkalmazkodás. A hackerek gyakran dinamikusan, valós időben vagy közel valós időben módosítják támadásaikat, így az 5G hálózat védelmének legalább ennyire alkalmazkodónak kell lennie. A sebesség egy másik létfontosságú követelmény, ami abban mutatkozik meg, hogy a hackerek tartózkodási idejét a rendszerben minimálisra csökkentsük. A harmadik az integráció. Az 5G-nek a lehető legtöbb különböző biztonsági eszközt és rendszert kell tudni integrálnia. A teljes biztonsági környezetből kialakított jelentések csökkentik a téves riasztások számát és a valódi fenyegetésekre való reagáláshoz szükséges időt. Az utolsó követelmény az automatizálás. Az automatizálás csökkenti a biztonsági csapatok növekvő munkaterhelését, mely alkalmas az ismétlődő támadások kezelésére. [12]

Az 5G legvonzóbb célpontjai a következők:

- a felhasználói eszközök;
- a hozzáférési hálózat;
- a maghálózat.



8. ábra Komplex biztonság [12]

Az 5G-ben a biztonság kezelése és hatékony működtetése nagyobb kihívást jelent az architektúra komplexitás miatt, amely magában foglalja a felhasználói eszközök biztonságát, a hozzáférési hálózat biztonságát, a felhő alapú biztonságot és a maghálózat biztonságát.

3.1 Felhasználói eszközök biztonsága

Az 5G hálózathoz csatlakozó és adatcserét végző eszközök növekvő száma számos kockázatot jelent. A felhasználói eszközök nagy népszerűségük miatt lehetnek célpontok. Napjainkban szinte minden ember rendelkezik mobiltelefonnal, tablettel, laptoppal, számítógéppel stb. Az 5G megnövelt adatátvitelt tesz lehetővé, melynek következtében a támadók több adathoz juthatnak hozzá. Továbbá az eszközök nyílt operációs rendszert és harmadik féltől származó appokat használnak, illetve többféle csatlakozási lehetőséget biztosítanak, mint a 2G, 3G, 4G, WiFi, Bluetooth technológiák, melyek tovább növelik a felhasználói eszközök sérülékenységeinek kockázatait.

Az 5G javítja a felhasználói és eszközadatok bizalmasságát és integritását. A felhasználói berendezés titkosítási algoritmusok segítségével támogatja az adatok bizalmas kezelését. Az eszközök a titkosítást a bázisállomás és saját maguk között a bázisállomás által küldött jelzésre aktiválják. A felhasználói berendezések a NEA (NR Encryption Algorithm) és NIA (NR Integrity Algorithm) titkosítási és integritás védelmi algoritmusokat használják. A felhasználói berendezésnek támogatnia kell az integritásvédelmet és a felhasználói adatok visszajátszásának védelmét az eszköz és a hálózati csomópontok között. A bizalmasság és integritás védelem opcionális tevékenységek mert, növelik a felhasználói berendezés és a hálózati csomópont feldolgozási terhelését. [13]

Az 5G hálózathoz való hozzáféréshez használt előfizetői hitelesítő adatok és kulcsok tárolására és feldolgozására olyan hardverelemeket kell használni, melyek garantálják az adatok sértetlenségét, bizalmasságát, elérhetetlenségét. A hosszú távú kulcsok soha ne legyenek elérhetők titkosítás nélkül a hardveren kívül. Minden olyan hitelesítési algoritmust, amely előfizettői hitelesítő adatokat használ, ezen a hardveren kell futtatni. [13]

A felhasználói eszközök ezenfelül különböző azonosítókat használnak. Ilyen azonosító a globális egyedi ideiglenes felhasználói eszköz azonosító, az előfizetés állandó és rejtett azonosító. Az előfizetői adatvédelemhez a kulcsokat és azonosítókat az USIM, azaz az univerzális előfizetői azonosító modul tartalmazza. Továbbá az 5G hálózat szolgáltatója felelős az előfizetői adatvédelemért, valamint az otthoni hálózat nyilvános kulcsának és a kulcs azonosítójának rendelkezésre bocsátásáért és frissítéséért.

Az 5G technológia mellett kialakuló e-SIM szolgáltatást is fontosnak tartom megemlíteni. Az e-SIM-mel rendelkező eszközök olyan eszközök, amelyekben a SIM kártya funkcióit az eszközbe integrált chip látja el. Az e-SIM több lehetőséget kínál, mint elődje. Az e-SIM egyik

biztonsági előnye, hogy nem lehet eltávolítani a készülékből, és annak ellopása vagy eltűnése esetén, az eszköz helye földrajzilag jól meghatározható. Ezenfelül az e-SIM több előfizetést is képes kezelni, amik internetkapcsolaton keresztül aktiválhatók. Ennek érdekében a legmodernebb biztonsági intézkedések révén védelmet biztosít a visszaélések ellen, ami vonatkozik az e-SIM profil nyilvános Wi-Fi hálózaton keresztüli letöltésére is.

3.2 A hozzáférési hálózat biztonsága

Az 5G hozzáférési hálózatának biztonsága hasonló az LTE-hez, amely tartalmaz titkosítást és integritásvédelmet a rádiós interfészen, valamint a bázisállomások és a maghálózat közötti IPSec-alagutakban. Az IPSec a legmodernebb forgalom titkosítás. Az összes forgalmi sík titkosítása megvédi a forgalmat a manipulációtól és lehallgatástól. Ezenkívül elrejti a maghálózatot, hogy megakadályozza, hogy hitelesítetlen elem csatlakozzon hozzá. A több ezer, esetleg több tízezer IPSec-kapcsolat kezelése a biztonsági átjárókhoz kihívást jelenthet.

A hozzáférési hálózatnak is meg kell őriznie az adatok bizalmasságát és integritását, ahogyan a felhasználói eszközöknek. A bizalmasság kezelésére az 5G gNB támogatja a továbbítás alatt lévő felhasználói adatok és a rádiós erőforrás-vezérlési jelzések titkosítását. Az ilyen titkosítási algoritmusok ugyanazok, mint amit a felhasználói berendezések használnak az adatok bizalmas kezelésére és integritás védelmére. A felhasználói és jelzési adatok integritását a csomópontoknak is garantálniuk kell, akárcsak a felhasználói berendezéseknek. A NIA0 algoritmus azonban nem ajánlott integritásvédelemre, mivel nem titkosít, és ezért szükségtelen többletterhelést jelent. Ezenfelül a bázisállomások biztosítják a rádiós erőforrás- vezérlési jelek integritásvédelmét is. [13]

Egy gNB telepítése és konfigurálása során, a 3GPP előírása alapján egy regisztrációs és hitelesítési hatóságnak engedélyeznie kell a gNB beállításokat és szoftverkonfigurációkat. Az üzemeltetési és felügyeleti rendszerek és a gNB közötti kommunikációt bizalmasan kell kezelni, és az integritás követelményének eleget téve kell védeni a jogosulatlan személyektől. Ezenkívül a szoftver- és adatmódosításokat engedélyezni kell a telepítés és használat előtt. Az érzékeny elemek védelme érdekében a rendszerindítási folyamatot biztonságos környezetben kell végrehajtani.

A gNB-n belüli kulcskezelés követelménye, hogy a gNB-telepítés minden olyan részét, amely titkosítatlan kulcsokat tárol vagy dolgoz fel, védeni kell a fizikai támadásoktól. Ha nincs fizikailag védve, akkor a gNB-t fizikailag biztonságos helyre kell helyezni. A gNB adatkezelésére is ezek az elvek az érvényesek. A biztonságos környezet logikailag

meghatározott a gNB-n belül, és biztosítja az összes érzékeny információ, illetve művelet védelmét, valamint titkosságát az illetéktelen hozzáféréssel szemben. A biztonságos környezet támogatja az érzékeny adatok biztonságos tárolását, az érzékeny funkciók végrehajtását, megköveteli a környezet integritását, és csak engedéllyel hozzáférhető.

3.3 A maghálózat biztonsága

Az 5G maghálózat szolgáltatás-alapú architektúrája felhő alapú megközelítéssel készült. Minden hálózati funkció a szolgáltatás alapú interfészen keresztül szolgáltatásként tárja fel képességét a hálózat számára, és ezt a képességet más hálózati funkciók újra felhasználják. Ezért az 5G maghálózat elemei között szolgáltatásbiztonsági kockázatok rejlenek.

A szolgáltatás-alapú architektúrája lehetővé teszi, hogy a magot különböző hálózati biztonsági zónákra tagoljuk, és a zónák közötti forgalmat a vezéreljük, felügyeljük, valamint annak adatintegritását érvényesítsük. Bizalmassági szabályokat is beállíthatunk minden zónához, ami jelentősen megnehezíti a fenyegetések terjedését egyik tartományról a másikra. A felhő alapú infrastruktúrája és dinamikus környezete új biztonsági kihívásokat jelent, amelyekre számos biztonsági intézkedéssel reagálni lehet. A virtualizációs réteg és a teljes felhőplatform-szoftver védelme, illetve az integritásának biztosítása a Virtual Network Functions (a továbbiakban: VNF) robusztus, biztonságtudatos megvalósítását igényli. A VNF-eket logikailag is el kell különíteni, sőt, ahol szükséges, fizikailag is el kell különíteni. A virtuális tűzfalak segítenek a terület biztonságában és a hálózati belső forgalom szűrésében. A kiválasztott forgalom és a tárolt adatok titkosítással is védhetők. [12]

Az 5G maghálózatban a támadó kihasználhatja a hálózati funkció azon sebezhetőségét, hogy feltörje azt, majd kérést kezdeményezhet a nyílt interfészről más hálózatok felé, ami anomáliát eredményezhet a hálózati funkció hozzáférési sorrendjében. Például a felhasználói eszköz regisztrációs hitelesítési eljárásában az AMF először hitelesítési kérelmet kezdeményez az AUSF[7]-hez (Authentication Server Function), amely ezután egy hitelesítési vektor létrehozását kéri az UDM[8]-től (Unified Data Management). Ha azonban egy támadó feltöri az AMF-et, közvetlenül felhívja az UDM felületét, hogy hitelesítési vektort hozzon létre, így ellopja a felhasználó hitelesítési információit. A támadó az egyes interfészek biztonsági rését is kihasználhatja. A támadó kihasználja a helytelen paraméterellenőrzések potenciális sebezhetőségét, ami hibát eredményez a visszaadott paraméterekben. Ezenfelül egy támadó

[7] Hitelesítési szerver funkció, amely egységes keretrendszert tesz lehetővé a 3GPP és nem 3GPP hozzáférésekhez.
[8] Egységes adatkezelési funkció, amely a számítási és tárolt adatokat szétválasztva tárolja.

nagyszámú hozzáférési kérelmet küldhet az 5G-maghálózatban lévő hálózati funkció nyílt interfészéhez, ami jelzővihart eredményez, ezért a szolgáltatás elérhetetlen lesz.

3.4 A hálózati szeletek biztonsága

A hálózati szeletelés felosztja a hálózatot elszigetelt szeletekre. Minden szelethez hozzá vannak rendelve a saját erőforrásai (sávszélesség, szolgáltatásminőség stb.), és egyedi biztonsági szabályzatokkal rendelkezik.

A hálózatszeletelésre vonatkozóan megkülönböztetünk a szelet életciklusára vonatkozó, a szeleten belüli és a szeletek közötti biztonsági réseket.

Egy hálózati szelet életciklusa az előkészületi fázistól a leszerelési fázisig tart, és a fázisok során eltérő célpontjai lehetnek a támadóknak. A fő támadási pont az előkészítési szakaszban a hálózati szelet sablon. A rosszul megtervezett, manipulált vagy helytelenül megvalósított hálózati szeletsablon (pl. tervezési hibák, befecskendezett rosszindulatú programok) az összes belőle épülő szeletet érinti. A konfigurálási fázis fő veszélyei közé tartozik a hamis szeletek létrehozása vagy a szeletek konfigurációjának megváltoztatása az aktiválás előtt vagy alatt. A harmadik fázis a szelet futásidejére vonatkozik. Ez a fázis a legkülönfélébb fenyegetéseknek van kitéve, ideértve a szolgáltatásmegtagadást (DoS), a teljesítmény elleni támadásokat, az adatok kitettségét és az adatvédelmi megszakításokat. A leszerelési fázis során érzékeny adatok kerülhetnek nyilvánosságra. [14]

A biztonsági intézkedéseket mind a négy fázisban ki kell alakítani, mert az egyik fázisban keletkezett sérülések károsíthatják a többi fázist. Ezenfelül a szeletsablonok integritására és titkosságára figyeljünk az átvitel és tárolás során. Hálózati szelet megszüntetése során meg kell semmisíteni az érzékeny adatokat, hiszen annak megismerése külső személy által károsíthatja a rendszerünket.

A szeleten belüli támadások eltérők, attól függően, hogy az adott szelet milyen szerepet tölt be a hálózatban. Ha a szelet több részszeletből álló láncként van meghatározva, akkor maguk az alszeletek és az alszeletek közötti kapcsolat is támadási pontokat jelent. Az alszeletek láncának általános biztonsági szintjét a leggyengébb alszelet adja. Az erőforrásokat és a hálózati funkciókat ért támadások károsíthatják az azokat fogyasztó szeleteket. A lehetséges támadások széles skálája történhet, beleértve a fizikai támadásokat, a szoftveres támadásokat és az általánosabb kibertámadásokat. [14]

A kommunikáció során a követelményeknek magukban kell foglalniuk a bizalmasságot, az integritást, az adatok hitelességét és a partnerek közötti kölcsönös hitelesítést.

A szeletek közötti biztonság a szeletek és szolgáltatások közötti kommunikáció biztonságára utal. Egy lehetséges támadási pont a különböző szeleteket fogyasztó szolgáltatások közötti interfész. Pontosabban, bizonyos szolgáltatások megtámadásával az ellenfél károsíthat más szolgáltatásokat, amelyek más szeleteken futnak. Ezenfelül a támadó megpróbálhat megtámadni egy kevésbé biztonságos szeletet, hogy megtámadjon egy biztonságosabb szeletet. Ha a szeletek közötti kommunikáció megengedett, a lehetséges fenyegetések közé tartozik az illetéktelen hozzáférés, a megosztott paraméterek kiszivárgása, a szeletek között továbbított érzékeny adatok. Az irányítási rendszer is támadási pontot jelent, melynek támadása során szintén más szeletekhez és azoknak a paramétereihez férhet hozzá a támadó. [14]

A szeletek közötti kommunikációt minimálisan csökkenteni kell, szigorú szabályok szerint kell meghatározni, és biztonságos csatornákon keresztül kell megvalósítani. A különálló hitelesítési, engedélyezési és hozzáférés-felügyeleti mechanizmusoknak függetlennek kell lenniük minden szeletnél.

Tehát hálózati szeletelés elősegíti a biztonságot, azonban a hálózaton lévő szeletek számának növekedése több konfigurációs hibához vezethet, ami hátrányosan befolyásolja a biztonságot.

3.5 Az 5G biztonságával foglalkozó fontosabb jogszabályok, dokumentumok

A támadások megelőzésére, a kockázatok csökkentésére törekedni kell. Ennek érdekében az Európai Unió Bizottsága elkészítette a „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” című eszköztárat. Mivel az 5G felhasználása sokkal szélesebb körű, újfajta adatok jelennek meg, a korábbi hálózatokkal ellentétben sokkal összetettebb megközelítés szükséges, ezért az Európai Unió Bizottsága az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) együttműködve készítette el ezt az ajánló csomagot. Az eszköztár konkrét javaslatokat tartalmaz a kockázatok minimalizálására. Szigorúbb javaslatokat tartalmaz többek közt a szabályozási környezet aktualizálására, a beszállítókkal kapcsolatos diverzifikációra, az operátorok védvonalainak megerősítésére, illetve a kiemelt kockázati besorolású beszállítók azonosítására.

Az Európai Bizottság által előterjesztett eszköztár stratégiai intézkedéseket és technikai intézkedéseket is tartalmaz. Az eszköztár által megfogalmazott stratégiai és technikai ajánlások az eszköztár következtetéseiben kerültek összefoglalásra. Az ott meghatározott, és az összes

tagállam által nemzeti szinten történő végrehajtásra javasolt legmagasabb hatékonyságú stratégiai és technikai intézkedések a következők:

- „A szabályozó hatóságok szerepének és hatáskörének megerősítése;
- A beszállítók kockázati profiljának felmérése, ennek következtében a magas kockázatúnak tekintett beszállítókra vonatkozó korlátozások alkalmazása;
- Minden üzemeltető megfelelő többszállítós stratégiával rendelkezzen az egyetlen szállítótól való jelentős függőség elkerülése vagy korlátozása érdekében;
- Sokszínű és fenntartható 5G ellátási lánc fenntartása a hosszú távú függőség elkerülése érdekében;
- Az üzemeltetőkre vonatkozó biztonsági követelmények szigorítása". [15]

Az ajánlások az Európai Elektronikus Hírközlési Kódex irányelvei alapján készültek el. Az Európai Elektronikus Hírközlési Kódex létrehozásáról, helyesebben a szükségessé váló módosítások kiadásáról az Európai Parlament és a Tanács (EU) 2018. december 11-én hatályba lépő 2018/1972 Irányelve rendelkezett.

Az Irányelv rendkívül szerteágazóan és részletesen taglalja az elektronikus hírközlés különböző területeihez tartozó szabályokat.

Az Európai Unió Irányelvei minden esetben rendelkeznek a nemzeti jogrendbe való átültetésük határidejéről. Jelen esetben a tagországok részére az Irányelv meghatározta, hogy 2020. december 21-ig fogadják el, és hirdessék ki „azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy az irányelv rendelkezéseinek megfeleljenek" [16], illetve ettől a dátumtól kezdve alkalmazniuk kell a rendelkezéseket.

Magyarország e kötelezettségnek az elektronikus hírközlésről szóló 2003. évi C. törvénynek (a továbbiakban: Eht), az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló irányelv átültetésének kötelezettségével összefüggő módosításáról szóló 2020. évi LXXXV. törvény kiadásával és 2020. december 21-től való hatályba léptetésével tett eleget.

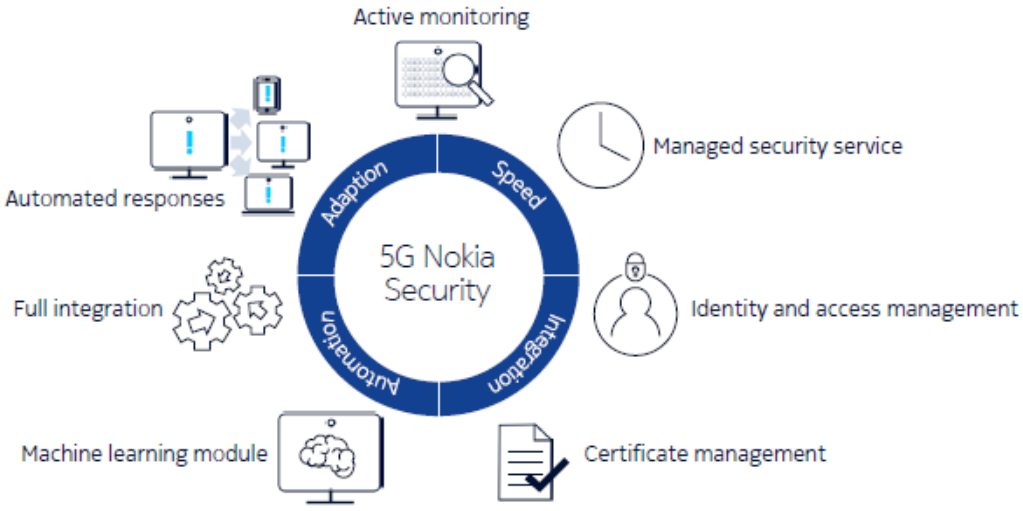
„Az Eht módosítása a fogyasztók védelmén túl olyan újdonságokat is tartalmaz, amelyek meggyorsítják a magyarországi 5G hálózatok fejlesztését és elterjedését. A módosítás többek között kiterjeszti a végfelhasználói jogokat és a spektrumgazdálkodást, illetve ösztönzi a beruházásokat". [17] Ezenfelül kiterjeszti a hírközlési szolgáltatások fogalmát, és olyan szolgáltatások is az Eht szabályozása alá kerülnek, mint a Skype, Viber stb. A fogyasztók védelmének érdekében a szolgáltatóknak át kellett alakítaniuk az általános szerződési

feltételeiket, melyek magukban foglalják a szerződéskötés, szerződésmódosítás, szerződés felmondása, szolgáltatóváltás, szolgáltatáscsomagok, számhordozás, tájékoztatás, adatvédelem területeit.

3.6 Összefoglalás

Az 5G biztonsági kialakítását nem lehet másolni a 4G (vagy régebbi generációk) biztonsági intézkedéseiről. Az egyéni biztonsági mechanizmusok helyett szisztematikus és elemző megközelítésre van szükség, mert az 5G rendszer támadható célpontjai sokkal szélesebb körűek, mint bármely más generáció esetében. Támadható célpontok a felhasználói eszközök, a hozzáférés és maghálózatok, az otthoni és külső hálózatok. Ezeknek a területeteknek a biztonsági kockázata csökkenthető vagy megszüntethető a megfelelő intézkedések betartásával. Ezenfelül nagyon fontos elem a biztonság szempontjából a felhasználók vagy munkavállalók biztonságtudatossága is. Általánosságban elmondható, hogy egy rendszer olyan erős, mint a leggyengébb láncszeme. Egy biztonságtudatos felhasználó tisztában van a biztonsági fenyegetésekkel és veszélyekkel, valamint mindent megtesz online biztonsága érdekében.

Az előzőekből és az alábbi ábrából jól látszik, hogy a biztonsági intézkedések rendszere is összetett.



9. ábra A teljes biztonság [12]

A támadások megelőzésére az Európai Unió, a 3GPP és Magyarország is elkészítette saját, az 5G biztonságával foglalkozó dokumentumait. Számos országban azonban még mindig folyik a munka a jogszabályok, az intézkedések tartalmának és hatályának meghatározásáról, illetve bizonyos esetekben még politikai döntéseket kell hozni ezzel kapcsolatban. Bár vannak még érvényes 5G előtti biztonsági megközelítések, azokat mindig újra kell vizsgálni, hogy

naprakészek legyenek az újonnan megjelenő fenyegetésekhez, hiszen az 5G szinte végtelen támadási lehetőséget biztosít. Magyarország a jogszabály alkotási kérdésben előre haladott, jelenleg az 5G bevezetési stádiumában az előre láthatóan szükséges szabályozások elkészültek.

4. AZ 5G KATONAI BEVEZETÉSÉNEK ÉS ALKALMAZÁSÁNAK LEHETŐSÉGEI

A verseny az 5G dominanciáért már javában zajlik. Az előző fejezetekből jól látható, hogy az 5G óriási lehetőségeket rejt magában, de komoly kihívások elé is állítja a technológiát alkalmazókat, így a NATO-t is. Ez egy összetett és gyorsan fejlődő technológia. Ha nem koordinálják a bevezetési folyamatokat a szövetségesek, azzal azt kockáztatják, hogy olyan 5G-technológiákat telepítenek, amelyek megfosztják az interoperabilitástól a rendszerüket és sebezhetővé teszik őket az ellenfeleik támadásaival szemben. A NATO-nak egy 5G-stratégiára van szüksége, hogy csökkentse vagy megszüntesse ezeket a kockázatokat, melyet a tagállamok a saját védelmi szférájukra tudják alkalmazni, illetve további szigorúbb intézkedéseket tudnak kialakítani. A szövetség azon képessége, hogy biztosítsa és megtartsa a technológiai csúcsot egy olyan harctérben, amelyet egyre inkább az adatigényes műveletek uralnak, döntő fontosságú lesz a küldetés sikere szempontjából.

4.1 A NATO szövetségesek álláspontja az 5G alkalmazásának tükrében

Az 5G és a következő generációs vezeték nélküli technológiák a katonai műveletekben is forradalmat eredményezhetnek, amely mindent megváltoztathat a kiképzéstől a logisztikán át a hadviselés harcászati, hadműveleti és hadászati dimenziójáig. Az 5G technológia lehetővé teszi a feltörekvő és zavaró technológiák (Emerging and disruptive technology, a továbbiakban: EDT) integrálását a katonai műveletekbe. Habár az 5G kulcsszerepet tölt be az EDT-k (pl.: mesterséges intelligencia, hiperszonikus járművek, rakéta technológia stb.) implementálásában, az 5G nem EDT, de mind a biztonság, mind pedig lehetőségek szempontjából érdekes terület.

A NATO szövetségesei között eltérések vannak az 5G beszerzéséhez és a műveleti keretekhez való hozzáállásukban, mellyel azt kockáztatják, hogy interoperabilitási hiányosságok keletkezhetnek a katonai potenciál kiaknázásában. Ennek ellenére egyes szövetségesek fontos nemzeti erőfeszítésekbe kezdtek, amelyek a katonai 5G körüli szélesebb körű koordináció alapjául szolgálhatnak. A tesztelésekből a következő elvek kerültek meghatározásra:

- az ellenálló képesség előtérbe helyezése;
- a szélessávú spektrummegosztás;
- az interoperabilitás fokozása;
- az ipari és szabályozási együttműködés.

Az 5G technológia felhasználásának széles köre (a katonaság, a biztonsági szolgálatok, a civil társadalom és a magánvállalatok) szerves részét képezi az ellenálló képesség és a hatékony megvalósítás eléréséhez. A redundáns struktúrák és rendszerek, különösen a kormányzati és kereskedelmi vállalatok között, csökkentik a rosszindulatú szereplők azon képességét, hogy immobilizálják ezeket a rendszereket.

A NATO-védelem szempontjából a spektrum-hozzáférés felosztása a kormányok és a civil társadalom között hatékonyabbnak bizonyulhat, mint ugyanazon spektrumrészekhez való kettős hozzáférés engedélyezése.

Az interoperabilitás fokozása talán a legfontosabb tényező az 5G katonai alkalmazásaiban, mely az egész szövetségre kiterjedő szabványosítástól függ. Mivel az 5G több csatlakozási lehetőséget, rugalmasságot, valamint nagyobb adatsebességet tesz lehetővé, így dinamikusabb és gördülékenyebb információáramlást eredményez a védelmi rendszerekben. Ez növeli a döntéshozatali folyamat sebességet, és csökkenti a válaszidőket válságos és válság előtti forgatókönyvekben.

A NATO-nak a tagállamaival közösen segítenie kell az 5G integrációját a szövetség haderőstruktúráiba és műveleteibe. A nemzeti kormányoknak a nyugati technológiát és a szabályozási diplomáciát kell kihasználniuk, hogy nemzetközi szabványokat hozzanak létre az 5G technológiára vonatkozóan. Nagyon fontos körülmény, hogy a technológia vezető szereplői nem nyugati, hanem kínai székhelyű cégek. Ez csökkenti a szövetségesek közötti interoperabilitást, és kockázatot jelent a hálózatok ellenálló képessége szempontjából. A mai napig az Egyesült Államok az egyetlen NATO-tagország, amely hatékony lépéseket tett annak érdekében, hogy korlátozza a kínai vállalatok hozzáférését az 5G hálózatához. Egyes szövetségesek (pl.: Olaszország, Németország) nem tiltották be a kínai 5G berendezések gyártóit, de már elkötelezték magukat a szigorúbb szabályozás mellett. Más NATO-tagországok (pl.: Egyesült Királyság, Csehország) álláspontja az idő előrehaladtával változott, és fokozatosan szigorodó álláspontot képvisel. A szövetségesek túlnyomó többsége nem tiltotta vagy korlátozta a kínai vállalatok szerepét az 5G infrastruktúrájában. Magyarország is abba a csoportba tartozik, aki már átvette a kínai 5G technológiát, és nem valószínű, hogy ebből visszalép.

Ezeknek a tényezőknek az 5G technológia fejlesztésébe való integrálása jobb pozíciókat biztosít a NATO számára az EDT-kben rejlő lehetőségek kiaknázásához és e rendszerek zavarokkal szembeni ellenálló képességének javításához. A szövetség nem tévesztheti szem

elől a katonai 5G bevezetéssel járó kockázatokat sem. Nemcsak ideiglenes intézkedésekre van szükség az 5G technológia biztonságos megvalósításához, mert a fejlődés nem áll meg, hanem a nyugati szövetségeseknek hosszú távú stratégiai előrelátással kell rendelkezniük ahhoz, hogy élen járjanak a 6G fejlesztésében.

4.2 Az 5G alkalmazási lehetőségei és kockázati tényezői a védelmi szféra keretein belül

A katonai alkalmazások igényei eltérnek a kereskedelmi 5G hálózatokétól. A katonai 5G hálózatokhoz olyan rendszerekre van szükség, amelyek önállóak, biztonságosak és könnyen csatlakoztathatók a meglévő felszerelésekhez. A nyílt szabványokon alapuló 5G hálózatok rugalmasságot, biztonságot és megbízhatóságot kínálnak ahhoz, hogy a különböző haderőnemek számos felhasználási területén alkalmazzák az 5G-t.

Macy Summers, a Blue Wireless Inc. elnöke szerint: „A több spektrális érzékelőadatok több forrásból való, valós időben történő taktikai integrációja meghatározza a harctéri kommunikáció jövőjét”. [18] Lehetőséget látok arra, hogy az 5G technológia megjelenésével olyan infokommunikációs rendszer kerülhet kiépítésre és alkalmazásra harcászati szinten, mely teljes mértékben felgyorsítja az információk továbbítását az ellenséges és saját erők helyzetéről, eszközeiről, létszámáról stb., ezzel is tovább gyorsítva a döntés előkészítést és végrehajtást. A technológia kis késleltetésének köszönhetően új típusú és nagyobb mennyiségű adatokkal (pl.: valós idejű képek és videók, az adott alegységek rendelkezésére álló készletek felmérése stb.) láthatja el a vezetési pontot akár egy harcjárműre szerelve, akár egy vagy több digitális katona eszközrendszerébe beépítve. Egy okosórával és a hordozható eszközökkel sok-sok információt lehet majd megosztani a katonák létfontosságú paramétereikről, mint például a pulzusszám, a vérnyomás és a fáradtság, egészen a földrajzi helyzetükig.

A modern drónoknak nagy távolságokat kell megtenniük, és potenciálisan több ezer más drónnal kell egy hálózatban működniük. Az 5G lehetővé teszi több eszköz támogatását és biztonságos, megbízható működését a látótávolságon túl. Az 5G-vel az AI-képes drónok fejlett érzékelési képességekkel rendelkeznek, és valós időben tudnak adatokat jelenteni, élő videót küldeni.

A ’telemedicine’ egy olyan modern gyakorlat, amely olyan technológiát foglal magában, amely a betegek és az orvosok különböző helyszíneken történő összekapcsolását szolgálja egészségtámogatás céljából. Az 5G segítségével elérhetővé válik távoli helyeken lévő csapatok orvosi ellátásának javítása. Lehetőség nyílik távoli, bonyolultabb operációk, vizsgálatok végrehajtására, mellyel a harcképesség tovább fenntartható.

Az 5G technológia nemcsak harcászati szinten hozhatna újdonságot. Az 5G lehetőséget nyújt olyan rendszer létrehozására is, melyben a rendszer minden eszköze kommunikál egymással, ezzel az információ áramlását gyorsítva, az információ rendelkezésre állását és azonnali elérését biztosítva. A jövőben elképzelhetőnek tartom akár tábori, akár stacioner 5G-s kommunikációs rendszerek megjelenését a Magyar Honvédségen belül is. Tábori szinten egy vezetési pont eszközeit kezelheti, foglalhatja egy rendszerbe, míg állandó 5G rendszerként okos laktanyák, okos irodák, okos létesítmények jelenhetnek meg. Okos laktanyák kialakításával, akár folyamatos adatot kaphatunk a fegyverszobában lévő fegyverektől kezdve a beléptető rendszerig.

Az 5G más adatigényes területeken, mint a kiképzés, a logisztika és a karbantartás is javíthatja a tevékenységek végrehajtását. A gyakorlótéren végrehajtott kiképzés során a katonák által viselt eszközökből kapott adatokból a gyakorlat elemzése és értékelése javíthatja a csapatmozgások végrehajtását. Emellett olyan kiterjesztett vagy virtuális valóságot használó környezet alakítható ki a laktanyákon belül, amely elősegíti a katona képzését.

A logisztika számára egy olyan rendszer kialakítását teheti lehetővé az 5G, ami a teljes ellátási láncot az elejétől a végéig láthatóvá teszi. Ezzel teljes felügyeletet biztosít a gyártás, a szállítás, a raktározás és karbantartás folyamataira. A szállítás során a gépjármű elhelyezkedését pontosan követhetjük. A raktárok teljesen emberi jelenlét nélkül üzemelhetnek, az ott lévő eszközöket távvezérléssel irányítva a raktárban lévő készleteket ezzel kezelve. Az érzékelőkkel pontos számokat kapunk a készletek mennyiségéről. A karbantartás előtt a rendszer rögzítené a valós eszközhasználatot, és a teljesítményadatok alapján figyelmeztetések jeleznék a karbantartás idejét, ezzel meghosszabbítva az eszközök élettartamát és csökkentve a befektetések költségét.

Egyes kutatók azt vizsgálják, hogy az 5G a radarhoz hasonlatosan használható-e azáltal, hogy a tárgyakról vagy emberekről való visszaverődésén alapuló képeket hoz létre, lehetővé téve a csapatok számára, hogy lássák az ellenséges katonákat, harcjárműveket a sarkok mögött vagy a sötét helyeken, ahol egyébként rejtve maradnának. A kutatás az 5G-alapú érzékelési technológiákat optikai kamerákkal és más eszközökkel is kombinálja, hogy minden időjárási körülmény között működjön.

Olyan kis, hordozható 5G egységet is elképzelhetőnek tartok, amelyet szinte bárhol le lehet dobni, majd aktiválni lehet, hogy egy adott földrajzi területen teljes 5G hálózatot biztosítson. Így az adott területen a meglévő fizikai infrastruktúrától függetlenül működhet, így ha

nincsenek mobiltornyok, akkor ez nem számít. Ugyanolyan hasznos lehet az ellenséges vonalak mögött tevékenykedő katonáknak, mint a hátországban maradt csapattoknak, akik távoli területeken végeznek például kutatást és mentést. A Private 5G Program ehhez hasonló rendszer fejlesztésén dolgozik.

A fentiek kockázati tényezői és a kockázatok elleni védelem kidolgozása során számos körülményt figyelembe kell venni. A technológiából adódóan az 5G hálózat által lefedett terület sűrűn, egymástól akár csak néhány tíz méterre lévő átjátszókat igényel. Ezek kiépítettségének helyzete alapvetően meghatározza az alkalmazhatóságot. Ezek az eszközök nem honvédségi tulajdonban vannak, de működőképességük fenntartása alapvető fontosságú, hiszen az esetleges meghibásodások a kialakított védelmi szféra rendszer működésképtelenségéhez vezethet. Ezenfelül az elérhetőségnek folyamatosnak kell lennie, mert a kapcsolat megszakadása az eszközzel súlyos károkat vagy hibákat okozhat az állományban, a döntéshozatali folyamatban, az eszközben stb.

4.3 Összefoglalás

Az 5G sokkal több lesz, többet jelent, mint gyors telefonhívások, különösen a védelmi szféra számára. Az 5G valójában valósággá teheti az információk azonnali és nagy mennyiségű áramlását, amiket videóból, hangból, érzékelőkből, célzásból, felderítésből stb. kapunk. Így bárki, akinek szüksége van az adatokra döntésének meghozatalában, könnyen és azonnal hozzáférhet.

Az 5G piacot olyan játékosok uralják, mint a Huawei, a Nokia és az Ericsson. Számos ország megkezdte az 5G integrációját a védelmi szférájába, és mivel a megvalósítás védelmi célokat szolgál, az adatok és a hálózat biztonsága, illetve az 5G beszállítók azonosítása kiemelten fontos. Az Egyesült Államok szilárdan kitart amellett, hogy nem vásárol hardvert és megoldásokat megbízhatatlan forrásokból, ahol az adatbiztonság aggodalomra ad okot.

Az 5G a védelmi szférában nem alkalmazható könnyen és gyorsan. Összehasonlítva a katonai, kereskedelmi és fogyasztói 5G általános elképzelésekkel, a technológia ma még gyerekcipőben jár. Az 5G katonai jövőjének megvalósításához időre, sok kísérletezésre, beruházásra és tervre van szükség. A tervnek magában kell foglalnia az 5G technológia fejlesztésének előmozdítását, az 5G előnyeinek és potenciális sebezhetőségeinek tesztelését, a magánszektorbeli partnerekkel való együttműködést, valamint az ipar aktív befolyásolását a politikák és szabványok kidolgozása és bevezetése során. Ezenfelül, mivel a katonai 5G technológia még életciklusának

korai szakaszában van, a technológiáról alapos ismeretekkel rendelkező munkaerő korlátozott, így a védelmi 5G infrastruktúra fejlesztése lassabb folyamat.

BEFEJEZŐ RÉSZ

A téma rövid összegzése, a lényeg kiemelése

Szakdolgozatomban megkíséreltem összefoglalni a mobilhálózatok generációit és az azokhoz kapcsolódó biztonsági témaköröket a legegyszerűbb és legérthetőbb módon. Ezenfelül az 5G jellemzői, biztonsági kérdései és alkalmazási lehetőségei kerültek ismertetésre részletesebben, mint a legaktuálisabb mobil technológia.

A korábbi mobilhálózat generációk bemutatásából látható, hogy a generációk miben tértek el egymástól. A mobilhálózati technológiák és a felhasználói igények rohamos fejlődése korábban nem látott bonyolultságú információs hálózatokat, új szolgáltatásokat, magasabb adatátviteli sebességet, új frekvenciasávokat eredményezett.

A mobilhálózatok fejlődésével egyszerre új biztonsági kockázatok megjelenését figyelhetjük meg, és ez az 5G megjelenése, bevezetése során is így van. A különbség a korábbi technológiákhoz képest egyszerűen annyi, hogy a soha nem látott fejlődési lehetőségek soha nem látott biztonsági kockázatokat is jelentenek, melyeket a dolgozatomban ismertetek. Ezért az 5G szabványosítását a 3GPP több kiadásra osztotta. A Release 15 és 16 írja le az rendszer alapfunkcióit és alapvető felhasználási eseteket. A Release 17 javítja a teljesítményt, és újabb eseteket tartalmaz.

Az 5G sokkal többet jelent, mint a meglévő 4G hálózatok teljesítményének növelését. Lehetőséget kínál a katonaságnak arra, hogy teljesen új használati eseteket fejlesszenek ki, és részesüljenek a civil világban elkezdődött újabb digitális átalakulásból. Ma a védelmi szektornak meg kell ragadnia ezt a lehetőséget, át kell alakítania kommunikációs rendszereit, és módosítania kell információs rendszereinek kialakítását.

Kijelenthető, hogy az 5G rendszerek biztonságos kialakítása szükséges és nélkülözhetetlen. A biztonság nem megfelelő ismerete helytelen védelmi, biztonsági tevékenységekhez vezethet, amik a mostani környezetünkben, szervezetünkben maradandó károkat okozhatnak. Tekintettel a biztonsági fenyegetések változó és összetett természetére, a kormányoknak, a szervezeteknek folyamatosan mérniük kell biztonsági helyzetüket és kockázati szintjüket, hogy ellenőrizzék, korlátozzák, és biztosítsák hálózataik, rendszereik, eszközeik megfelelő működését.

Mivel az 5G szabványosítása befejeződött érdemes elgondolkodni mi jön majd utána, milyen lehet majd a 6G. Mint minden egymást követő mobilhálózat generációnál, a sebesség és késleltetés lehet a legmeghatározóbb különbség az 5G és 6G között. Arra számíthatunk, hogy a 6G többszörös gyorsaságú lesz, akár terabytos sebességet elérve, illetve megközelítheti a rádióspektrum felső határát. A következő generációs mobilhálózatok valamikor egy legmagasabb szintet elérnek majd és nem biztos, hogy mindig újdonságot fognak jelenteni.

A témával kapcsolatos jövőbeni szándékok

Lehetőséget látok arra, hogy a téma alaposabb kidolgozásával, továbbá egyéb, az 5G-hez kapcsolódó témakörök feldolgozásával további kutató munkát végezzek. Hasonló gondolatmenet mentén bármely témakör vonatkozásában elképzelhetőnek látom ilyen elemzés elvégzését. Így tehát más szakirányokhoz kapcsolódó téma vonatkozásában is lehetőséget látok akár hasonló anyag elkészítésére, vagy akár ennél mélyebb elemzés elkészítésére is. Elképzelhetőnek tartom, hogy a 6G megjelenésével hasonló kutatást készítsek további tanulmányaimhoz.

IRODALOMJEGYZÉK

3GPP TR 21.916 V16.1.0 (2022-01) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 16 Description; Summary of Rel-16 Work Items (Release 16)

3GPP TR 21.917 V0.1.0 (2021-11) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 17 Description; Summary of Rel-17 Work Items (Release 17)

3GPP TR 22.861 V14.1.0 (2016-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers for Massive Internet of Things; Stage 1 (Release 14)

3GPP TR 22.862 V14.1.0 (2016-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers for Critical Communications; Stage 1 (Release 14)

3GPP TR 22.863 V14.1.0 (2016-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers - Enhanced Mobile Broadband; Stage 1 (Release 14)

3GPP TR 22.864 V15.0.0 (2016-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers - Network Operation; Stage 1 (Release 15)

3GPP TS 22.261 V15.9.0 (2021-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for the 5G system; Stage 1 (Release 15)

3GPP TS 22.368 V15.0.0 (2019-07) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC); Stage 1 (Release 15)

5G a közbiztonságért, https://www.critical-communications-world.com/media/16433/10-philippe-agard.pdf [Online]. [Letöltés dátuma: 2022.03.13]

5G hálózatok és a Release 15, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/ITU-ASP-CoE-Training-on-/session7_5G%20networks%20and%203GPP%20release%2015.pdf [Online]. [Letöltés dátuma: 2022.03.13]

2003. évi C. törvény az elektronikus hírközlésről

2013. évi. L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2017. évi LXXXVIII. törvény a 2003. évi C. törvény módosításáról

109/2007. (V. 15.) Korm. rendelet az egységes digitális rádió-távközlő rendszerről

346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról

1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiája

A 3GPP 15., 16. és 17. kiadásának bemutatása, https://5g.security/5g-technology/5g-3gpp-releases-15-16-17/ [Online]. [Letöltés dátuma: 2022.03.13]

A 3GPP 16. és 17. kiadásának áttekintése, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-nr-evolution [Online]. [Letöltés dátuma: 2022.03.13]

A 3GPP-ről, https://www.3gpp.org/about-3gpp?fbclid=IwAR0ms9B06GT0Mej_liPoD1kZRcqm9VsI6-brdsNtImUDMCwus7Q8d6p6fLs [Online]. [Letöltés dátuma: 2022.03.13]

A következő generációs vezeték nélküli technológia harctéri forradalmat ígér, https://www.defenseone.com/ideas/2020/08/nato-must-move-out-smartly-5g/167687/ [Online]. [Letöltés dátuma: 2022.03.13]

A mobilhálózatok fejlődése, https://medium.com/@Matt.Bartlett/the-evolution-of-mobile-wireless-technology-from-0g-to-5g-cf98c80e2323 [Online]. [Letöltés dátuma: 2022.03.13]

A Release 15, https://www.3gpp.org/release-15 [Online]. [Letöltés dátuma: 2022.03.13]

A Release 16: Biztonság és RAN, https://www.ericsson.com/en/blog/2021/4/3gpp-release-16-5g-phase-2-security-ran [Online]. [Letöltés dátuma: 2022.03.13]

A Release 17, https://www.ericsson.com/en/blog/2019/12/3gpp-rel-17 [Online]. [Letöltés dátuma: 2022.03.13]

A továbbfejlesztett mobil szélessáv, https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/ [Online]. [Letöltés dátuma: 2022.03.13]

Az 5G szabványok fejlesztései a Release 15-ben és azon túl, https://www.atis.org/wp-content/uploads/2020/02/5g-slides7312019.pdf [Online]. [Letöltés dátuma: 2022.03.13]

Az 5G szabványok következő fejezete, a Release 17, https://www.qualcomm.com/news/onq/2019/12/13/3gpp-charts-next-chapter-5g-standards [Online]. [Letöltés dátuma: 2022.03.13]

Az 5G az euro-atlanti térség szövetségesévé tétele, https://cepa.org/making-5g-an-ally-of-the-euro-atlantic-area/ [Online]. [Letöltés dátuma: 2022.03.13]

Az 5G-ben rejlő lehetőségeket a NATO számára, https://www.ncia.nato.int/about-us/newsroom/nato-tech-agency-explores-the-potential-of-5g-for-the-alliance.html [Online]. [Letöltés dátuma: 2022.03.13]

Az IMT-2000 szempontjai, https://www.itu.int/en/ITU-T/imt-2000/Pages/default.aspx [Online]. [Letöltés dátuma:2022.03.13]

Az ITU az IMT-2020 felé, https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx [Online]. [Letöltés dátuma: 2022.03.13]

Az ipari automatizálás, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-tsn-integration-for-industrial-automation [Online]. [Letöltés dátuma: 2022.03.13]

Cybersecurity of 5G networks EU Toolbox of risk mitigating measures [Offline] [pdf]

Elkészült az első 5G-szabvány, https://www.qualcomm.com/news/onq/2018/03/21/first-5g-standard-complete-so-whats-next [Online]. [Letöltés dátuma: 2022.03.13]

Hibák az LTE protokollokban, https://nki.gov.hu/it-biztonsag/hirek/komoly-biztonsagi-hibakat-fedeztek-fel-a-4g-lte-protokollokban/ [Online]. [Letöltés dátuma: 2022.03.13]

Jobbágy Szabolcs és Serege Gábor, „Az egységes készenléti digitélis trönkölt rádiórendszer TETRA ÉS TETRAPOL jellemzői, sajátosságai”, https://www.puskashirbaje.hu/index_html_files/Kommunikacio_2003-NSZTK.pdf [Online]. [Letöltés dátuma: 2022.03.13]

Kuris Zoltán, „Az egységes digitális rádiórendszer (EDR) alkalmazásának lehetőségei a rendészeti szerveknél” *Hadmérnök,* V. évfolyam 2. szám 2010 június [Online]

LTE biztonság, https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf [Online]. [Letöltés dátuma: 2022.03.13]

Massive Machine Type Communications, https://blogs.cisco.com/sp/3services5gmassmachine [Online]. [Letöltés dátuma: 2022.03.13]

Minimális műszaki teljesítménykövetelmények az IMT-2020-hoz, https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Documents/S01-1_Requirements%20for%20IMT-2020_Rev.pdf [Online]. [Letöltés dátuma: 2022.03.13]

Mit jelent az IMT?, https://www.itu.int/en/ITU-R/Documents/ITU-R-FAQ-IMT.pdf [Online]. [Letöltés dátuma: 2022.03.13]

NATO és az 5G, https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html [Online]. [Letöltés dátuma: 2022.03.13]

Katonai 5G kommunikáció, https://www.militaryaerospace.com/rf-analog/article/14188341/military-5g-communications [Online]. [Letöltés dátuma: 2022.03.13]

Kína, 5G és NATO biztonság, https://www.gmfus.org/news/china-5g-and-nato-security [Online]. [Letöltés dátuma: 2022.03.13]

Project Report CS 649: NETWORK SECURITY GSM and UMTS Security Under Guidance of Prof. Bernard Menezes [Offline]. [pdf]

The International Engineering Consortium – Global System for Mobile Communication (GSM) [Offline]. [pdf]

Workshop NATO Military 5G/NGN vision and strategy. [Konferencia]

HIVATKOZÁSOK JEGYZÉKE

[1] Az 5G, https://5g.hu/hu/mi-az-5g [Online]. [Letöltés dátuma: 2022.03.13]

[2] Így fejlődött a mobiltechnológia, https://www.yettel.hu/sajto/kozlemeny/25-ev-evfordulo [Online]. [Letöltés dátuma: 2022.03.13]

[3] 5G a kiberbűnözők kezében, https://www.digitalhungary.hu/e-volution/Veszelyes-fegyver-lehet-az-5G-a-kiberbunozok-kezeben/9463/ [Online]. [Letöltés dátuma: 2022.03.13]

[4] Tóth Tamás, „A mobilhálózatok technológiai fejlődsétörténete – az analóg hangátviteltől az 5G-hálózatokig” https://epa.oszk.hu/02500/02538/00031/pdf/EPA02538_nemzetbiztonsagi_szemle_2019_04_044-060.pdf [Online]. [Letöltés dátuma: 2022.03.13]

[5] 3GPP partnerek, https://www.3gpp.org/about-3gpp/partners [Online]. [Letöltés dátuma: 2022.03.13]

[6] Az LTE Advanced, https://pcworld.hu/tippek/minden-amit-tudnod-kell-az-lte-advancedrol-159332.html [Online]. [Letöltés dátuma: 2022.03.13]

[7] 5G szabványosítása, http://www.mszt.hu/web/guest/5g-informaciok [Online]. [Letöltés dátuma: 2022.03.13]

[8] Az 5G követelmények vizsgálata, https://www.3gpp.org/news-events/1786-5g_reqs_sa1 [Online]. [Letöltés dátuma: 2022.03.13]

[9] 3GPP TR 21.915 V15.0.0 (2019-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 15 Description; Summary of Rel-15 Work Items (Release 15)

[10] Az 5G 16. és 17. kiadása, https://d1p0gxnqcu0lvz.cloudfront.net/documents/Nokia_Bell_Labs_5G_Releases_16_and_17_in_3GPP_White_Paper_1_EN.pdf [Online]. [Letöltés dátuma: 2022.03.13]

[11] Az 5G Advanced felé, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-evolution-toward-5g-advanced [Online]. [Letöltés dátuma: 2022.03.13]

[12] NOKIA 5G security for government [Offline] [pdf]

[13] 3GPP TS 33.501 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects, Security architecture and procedures for 5G system (Release 17)

[14] Az 5G hálózatszeletelése, https://ieeexplore.ieee.org/document/9099823?denied= [Online]. [Letöltés dátuma:2022.03.13]

[15] Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity [Offline] [pdf]

[16] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1972 IRÁNYELVE, 2018. december 11.*

[17] Az Elektronikus Hírközlési törvény módosítás, https://home.kpmg/hu/hu/home/media/press-releases/2020/07/lealdozott-az-emeltdijas-hivasokkal-valo-visszaeleseknek.html [Online]. [Letöltés dátuma:2022.03.13]

[18] A taktikai 5G hálózat, https://www.defenseworld.net/interview/109/Tactical_5G_Networking_Will_Define_the_Future_of_Battlefield_Communications#.Yi41j3rMLIX [Online]. [Letöltés dátuma: 2022.03.13]

RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Idegen nyelvű megfelelő	Magyar nyelvű megfelelő
3GPP	3rd Generation Partnership Project	3. Generációs Partnerségi Projekt
AMF	Core Access and Mobility Management Function	Hozzáférés és Mobilitás Menedzsment Funkció
AUSF	Authentication Server Function	Hitelesítési Szerver Funkció
eMBB	Enhanced Mobile Broadband	Továbbfejlesztett Mobil Szélessáv
ENISA	European Union Agency for Cybersecurity	Európai Uniós Kiberbiztonsági Ügynökség
ETSI	European Telecommunications Standards Institute	Európai Távközlési Szabványosítási Intézet
FM	Frequency modulation	Frekvencia moduláció
gNB	gNodeB	Bázisállomás
IAB	Integrated Access and Backhaul	IntegráltHhozzáférés és Backhaul
IEEE	Institute of Electrical and Electronics Engineers	Villamos és Elektronikus Mérnökök Intézete
ITU	International Telecommunication Union	Nemzetközi Távközlési Egyesület
MIMO	Multiple Input and Multiple Output	Többszörös Bemenet és Többszörös Kimenet
mMTC	Massive Machine Type Communication	Masszív Gép Típusú Kommunikáció
mTRP	Multiple Transmission and Reception	Többszörös Átviteli és Vételi Pont
NR-U	New Radio Unlicenced	Licenc Nélküli Spektrum
NSA	Non-Stand Alone	Nem Önálló
NTN	Non-Terrestrial Network	Nem Földi Hálózat
OFDM	Orthogonal Frequency Division Multiplexing	Ortogonális Frekvenciaosztású Többszörös Hozzáférés
SA	Stand Alone	Önálló
UDM	Unified Data Management	Egységes Adatkezelési Funkció
UPF	User Plane Function	Felhasználói Sík Funkció
URLLC	Ultra Reliable Low Latency Communication	Ultra Megbízható Alacsony Késleltetésű Kommunikáció
VNF	Virtual Network Functions	Virtuális Hálózati Funkció

ÁBRÁK, TÁBLÁZATOK JEGYZÉKE

A szakdolgozatban szereplő ábrák

1. ábra A mobilhálózatok generációnak fejlődése az adatátviteli sebesség tükrében

2. ábra A felhasználói esetek csoportjai

3. ábra NSA architektúra

4. ábra SA architektúra

5. ábra Az 5G rendszer felépítése

6. ábra A frekvenciatartomány kiterjesztése

7. ábra A kiadások időpontjai

8. ábra Komplex biztonság

9. ábra A teljes biztonság

A szakdolgozatban szereplő táblázatok

1. táblázat Az 5G frekvenciatartományai

2. táblázat Az 5G egyéb jellemzői

3. függelék

A konzultációkon történő részvétel igazolása

A konzultációkon történő részvétel igazolása
(szakdolgozathoz/diplomamunkához)

A hallgató neve:	Kiss Bence
A hallgató Neptun-kódja:	Y6UKO4
Szak, szakirány megnevezése:	Katonai üzemeltetés szak, Híradó szakirány
Képzési szint (alap-/mesterképzés):	alapképzés
Munkarend (levelező/nappali):	nappali
A dolgozat címe:	Az 5. generációs mobilhálózatok jellemzői, biztonsági aspektusai és alkalmazási lehetőségei a védelmi szférában.
A dolgozat konzulensének neve:	Dr. Jobbágy Szabolcs
A konzulens munkahelye,	NKE HHK Híradó Tanszék, egyetemi adjunktus

1. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2021. szeptember 29. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. *(Aláhúzni!)*

   Budapest, 2021. év szeptember hó 29. nap

   .....
   Konzulens aláírása

2. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2021. november 25. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)

   Budapest, 2021. év november hó 25. nap

   .....
   Konzulens aláírása

3. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2022. január 18. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)

   Budapest, 2022. év január hó 18. nap

   .....
   Konzulens aláírása

4. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2022. február 03. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)

Budapest, 2022. év február hó 03. nap

.....

Konzulens aláírása

5. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2022. február 23. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)

Budapest, 2022. év február hó 23. nap

.....

Konzulens aláírása

6. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2022. március 10. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)

Budapest, 2022. év március hó 10. nap

.....

Konzulens aláírása

7. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2022. március 16. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)

Budapest, 2022. év március hó 16. nap

.....

Konzulens aláírása

8. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2022. március 23. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)

Budapest, 2022. év március hó 23. nap

.....

Konzulens aláírása

Készült 2 eredeti példányban.

A hallgatónak a témajelentkezés véglegesítését követően, a szakdolgozat/diplomamunka elkészítése során legalább három alkalommal kell konzultáción –aláírással is igazoltan - részt vennie. Ennek hiányában a szakdolgozat/diplomamunka bírálatra, illetve védésre nem bocsátható.

4. függelék

Konzulensi vélemény

Konzulensi vélemény
(szakdolgozathoz/diplomamunkához)

A hallgató neve:	Kiss Bence
A hallgató Neptun-kódja:	Y6UKO4
Szak, szakirány megnevezése:	Katonai üzemeltetés szak, Híradó szakirány
Képzési szint (alap-/mesterképzés):	alapképzés
Munkarend (levelező/nappali):	nappali
A dolgozat címe:	Az 5. generációs mobilhálózatok jellemzői, biztonsági aspektusai és alkalmazási lehetőségei a védelmi
A dolgozat konzulensének neve:	Dr. Jobbágy Szabolcs
A konzulens munkahelye,	NKE HHK Híradó Tanszék, egyetemi adjunktus

Szöveges értékelés, megjegyzés (kötelező, minimum 1000 karakter):

A hallgató által választott téma aktualitása vitathatatlan, hiszen a 21. század digitális-információs társadalmának keretei között a különböző infokommunikációs technológiák robbanásszerű fejlődésének lehetünk szemtanúi és részesei. Ebben a technológiai forradalomban élen járnak a különböző vezeték nélküli mobil kommunikációs technológiák is, melyek közül napjainkra az egyik legnagyobb hatást az 5. generációs mobil kommunikációs technológiai képezi. Annak ellenére, hogy teljeskörű térhódítása még meg sem történt, a különböző nemzetközi szakmai szervezetek és szakemberek már a következő nagy technológiai mérföldkő, a 6G megalkotásán fáradoznak. Az 5G olyan új távlatokat nyit meg az infokommunikációban, melyre korábban még soha nem volt példa. Főbb alkalmazási területei közé a különböző digitalizált valóságok, az önvezető autók közötti kommunikáció, a telemedicina vagy az okos eszközök és alkalmazások technológiai platformjának a biztosítása sorolható. Noha korábban a védelmi szféra jeleskedett a különböző újítások megalkotásában, és ebből a szegmensből adaptálódtak az újítások a civil szférába, napjainkban ezek a folyamatok megfordultak, a védelmi szférában történő alkalmazhatóság vizsgálata képezheti vagy kell, hogy képezze a különböző kutatások egyik legfontosabb tárgyát.

A hallgató meglátva mindezt a logikai vezérfonalat, vizsgálati szükségességet, dolgozatában szisztematikusan áttekinti az egyes generációkat képviselő technológiai implementációk főbb sajátosságait, illetve az azokban rejlő biztonsági kockázatokat, sérülékenységeket,

sebezhetőségeket, fenyegetéseket. Munkájában a vállalt feladattal összhangban a fő hangsúlyt az 5G NR technológia szélesebb körű vizsgálatára helyezi, górcső alá véve annak valamennyi meghatározó szegmensét a kommunikáció biztonságának szemüvegén keresztül. Dolgozatának másik hasonló jelentőséggel bíró fejezete az 5G technológia védelmi szférában történő alkalmazhatóságának vizsgálata, melynek keretében a Magyar Honvédség, mint NATO tagország tekintetében egy egységes nemzetközi keretrendszerbe helyezve fogalmaz meg jövőbeli ajánlásokat a lehetséges implementációkra.

Összeségében megállapítom, hogy a hallgató eleget tett a részére kiadott feladatlapon meghatározott feladatok teljesítésének. Az elkészített szakdolgozat megfelel a Tanulmányi és Vizsgaszabályzatban meghatározott tartalmi és formai követelményeknek, annak egyes fejezetei logikusan épülnek egymásra követve a feladatlap pontjainak vezérfonalát, a megfelelő szakirodalmat a kellő mélységében tekintette át, a dolgozat szerkezetileg jól tagolt, az ábrák és képek növelik annak színvonalát, fokozva annak áttekinthetőégét és segítve a tartalmi mondanivaló megértését, mely szakmailag megalapozott, olvasmányos, érthető megfogalmazású. A dolgozat témája, a feldolgozott kérdéskörök kapcsolódnak a Katonai üzemeltetés alapképzési szak, Híradó szakirány képzési portfóliójában feldolgozott ismeretanyagokhoz. Plágium gyanúja nem merült fel, a felhasznált irodalmak, átvett anyagok korrekt hivatkozása megtörtént.

Mindezekre tekintettel javaslom a hallgató által elkészített dolgozat szakdolgozatként történő benyújtását, annak bírálatra bocsátását és védését.

A Tanulmányi és Vizsgaszabályzat 5. számú melléklet II/5. pontjában meghatározott vizsgálatot elvégeztem.

A dolgozat a hallgató saját szellemi terméke, szerzői jogsértés/plágium gyanúja nem merült fel. / A dolgozattal kapcsolatban szerzői jogsértés/plágium gyanúja merül fel az alábbiak szerint: *(Aláhúzni, kitölteni!)*

A dolgozatot védésre javaslom / nem javaslom. *(Aláhúzni!)*

Budapest, 2022. év március hó 22. nap

.....

Konzulens aláírása

Készült 2 eredeti példányban.

5. függelék

Szerzői jogi nyilatkozat
(szakdolgozathoz / diplomamunkához
a Neptun-rendszer felületén)

Büntetőjogi felelősségem tudatában nyilatkozom, hogy a benyújtott jelen szakdolgozat/diplomamunka saját szellemi tevékenységem eredménye, az abban hivatkozott nyomtatott és elektronikus szakirodalom felhasználása a szerzői jogokra vonatkozó jogszabályoknak megfelelően történt, a benne foglaltak más személyek jogszabályban rögzített jogait nem sértik.

Szerzői jogi nyilatkozat
(szakdolgozathoz / diplomamunkához
papír alapú)

Alulírott Kiss Bence (NEPTUN-kód: Y6UKO4) büntetőjogi felelősségem tudatában kijelentem, hogy „Az 5. generációs mobilhálózatok jellemzői, biztonsági aspektusai és alkalmazási lehetőségei a védelmi szférában" című, a Nemzeti Közszolgálati Egyetem Katonai üzemeltetés szak, Híradó szakirány képzésén benyújtott jelen szakdolgozat/diplomamunka saját szellemi tevékenységem eredménye, az abban hivatkozott nyomtatott és elektronikus szakirodalom felhasználása a szerzői jogokra vonatkozó jogszabályoknak megfelelően történt, a benne foglaltak más személyek jogszabályban rögzített jogait nem sértik.

Budapest, 2022. év március hó 22. nap

Kiss Bence
.....

Hallgató aláírása

6. függelék

Felhasználási nyilatkozat
(szakdolgozathoz / diplomamunkához)

A hallgató neve:	Kiss Bence
Kar:	Hadtudományi és Honvédtisztképző Kar
Oktatási szervezeti egység:	Híradó Tanszék
Szak, szakirány:	Katonai üzemeltetés szak, Híradó szakirány
A dolgozat címe:	Az 5. generációs mobilhálózatok jellemzői, biztonsági aspektusai és alkalmazási lehetőségei a védelmi szférában.
A dolgozat elkészítésének éve:	2022

I.* Alulírott, mint a szakdolgozat/diplomamunka szerzője, a szerzői jog kizárólagos jogosultjaként

hozzájárulok,
nem járulok hozzá,

hogy a szakdolgozatom/diplomamunkám példányát más személyek tanulmányaik, kutatásaik során – a hivatkozási előírások betartásával – felhasználják.

„Hozzájárulok" válasz esetén a II. pont kitöltése kötelező.

II.* Alulírott, mint a szakdolgozat/diplomamunka szerzője, a szerző jog kizárólagos jogosultjaként hozzájárulok, hogy a dolgozatom teljes szövegének elektronikus változatát a Nemzeti Közszolgálati Egyetem Egyetemi Központi Könyvtár és Levéltár által működtetett egyetemi repozitórium nyilvánosan szolgáltassa:

korlátlan hozzáféréssel (teljes nyilvánossággal az interneten elérhetően)*
korlátozott hozzáféréssel (korlátozott nyilvánossággal, egyetemi IP címről egyedi felhasználói azonosítóval)*

III. *Alulírott, mint a szakdolgozat/diplomamunka szerzője, a szerzői jog kizárólagos jogosultjaként ***nem járulok hozzá***, hogy a dolgozatom teljes szövegét a Nemzeti Közszolgálati Egyetem Egyetemi Központi Könyvtár és Levéltár nyilvánosan szolgáltassa.*

Budapest, 2022. év március hó 22. nap

Kiss Bence
.....

Hallgató aláírása

Megjegyzés: A *-gal jelölt részt aláhúzssal kérjük jelölni. Amennyiben a szakdolgozat / diplomamunka felhasználói nyilatkozatának kitöltése elmarad vagy hiányosan történik, abban az esetben a szakdolgozat / diplomamunkába betekintési lehetőség nincs.