ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

BORSOS DÖNÍZ

IoT technológiák alkalmazásának lehetőségei a személy- és vagyonvédelem területén

Témavezető: Prof. Em. Dr. Berek Lajos

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2026. március 08.

TARTALOMJEGYZÉK

BEVEZETÉS

Az elmúlt évtizedben az IoT-alapú (Internet of Things – Dolgok Internete) megoldások rohamos fejlődése [1][2][3] számottevően átalakította a műszaki infrastruktúrák működését [4] és a különböző szolgáltatások technológiai hátterét [5], beleértve a biztonságtechnikai megoldásokat is. A megjelent új rendszerarchitektúrák lehetővé tették a fizikai környezet állandó monitorozását, az érzékelőinformációk valós idejű továbbítását, valamint a folyamatos távfelügyeletet és a teljesen automatizált működést. [6] A nagy kiterjedésű hálózatok kialakítását szolgáló technológiák új dimenziót nyitottak meg [7] a vezetéknélküli infrastruktúrák kialakításában és a vezetékes megoldások kiváltásában.

Ez a fejlődési irány, a személy- és vagyonvédelemben is jelentős változásokat hozott. A különböző detektáló- és jelzőrendszerek, valamint a távfelügyeleti rendszerek egyre gyakrabban támaszkodnak valamilyen IoT-kommunikációra. [8] Alkalmazásuk előnyös lehet kiterjedt objektumok és elszigetelt területek felügyeletekor [9] vagy utólagos telepítés esetén. Ezzel párhuzamosan, ahogy bővültek a technológiai lehetőségek, új típusú kérdések és kockázatok [10] jelentek meg.

A korábbi, jellemzően zárt, dedikált kommunikációra épülő személy- és vagyonvédelmi rendszerek helyére egyre több, nyílt szabványra épülő, vezetéknélküli infrastruktúra kerül. A rugalmasságot és az egyszerű integrálhatóságot biztosító megoldások a rendszerek komplexitásnövekedésével járnak és a kockázati tényezők számát is növelik. Ez azt eredményezi, hogy az új rendszerek a korábbinál átfogóbb megközelítéseket igényelnek. Személy- és vagyonvédelmi rendszerekben az adatátvitel nem egyszerűen statisztikai célú, mint például egy fogyasztásmérés esetén, hanem közvetlenül hatással van a rendszerszintű kiértékelésre és döntéshozatalra [11], például egy behatolásdetektálás esetén.

Közel tíz éve foglalkozom IoT-alapú kommunikációs rendszerek tervezésével, fejlesztésével és elemzésével, ezen belül kiemelten a LoRaWAN technológiával, de munkásságom kiterjed az ipari kommunikációs megoldásokra, az Ipar 4.0 koncepcióhoz kapcsolódó infrastruktúrákra, kritikus infrastruktúrák vizsgálatára és az okos város koncepció kapcsolataira. A korábbi kutatási és fejlesztési tevékenységeim tapasztalatai rámutattak arra, hogy a kommunikációs működőképesség, a specifikációs megfelelőség és a rendszer tényleges megbízhatósága nem minden esetben esik egybe.

Mindezek alapján megállapítható, hogy szükség van egy olyan átfogó megközelítésre, amely az IoT-technológiák személy- és vagyonvédelmi alkalmazhatóságát a technológiai sajátosságok, a működési korlátok és az életciklus-menedzsment kérdéseinek integrált vizsgálatával értelmezi.

A tudományos probléma megfogalmazás

Az IoT-alapú rendszerek nem csak ipari területen vagy a mindennapi élet részeként jelentek meg, hanem a személy- és vagyonvédelem területén is meghatározó számban jelen vannak. Ezek, a főleg érzékelőalapú megoldások lehetővé teszik a decentralizált adatgyűjtést és a nagykiterjedésű objektumok rugalmas felügyeletét. Az eltérő LPWAN (Low Power Wide Area Network: Alacsony energiafogyasztású, nagy kiterjedésű hálózatok) technológiák, műszaki szempontból alkalmasak kis adatok, állapot vagy riasztási funkciók továbbítására, így megjelentek személy- és vagyonvédelmi rendszerekben is.

Az IoT elterjedése azonban megelőzte annak biztonságtechnikatudományi aspektusú rendszerszintű vizsgálatát. Tehát az igény megjelent, amit a piac ki is szolgált, de a szakirodalom jelentős része kommunikációs paraméterekre, energiafogyasztás optimalizálására, protokollszintű leírásokra és vizsgálatokra, valamint hálózati felépítésre, esetlegesen információbiztonsági kérdésekre összpontosít. Ezzel szemben, elmarad az IoT végpontok megbízhatósági és kockázati elemzése személy- és vagyonvédelmi alkalmazások kontextusában. Nem vizsgált az IoT sajátosságokból adódó korlátok tényleges védelmi érintettsége és hatása.

A tudományos probléma másik vetülete az IoT végpontok életciklusának teljeskörű kezelése. Az elérhető tudományos publikációk és műszaki dokumentációk jellemzően a telepítésre és üzemeltetésre koncentrálnak, eközben az eszközök életciklus-lezárásának fizikai és logikai kezelése nem jelenik meg egységesített, kidolgozott formában. A szakirodalomban találhatók utalások a kivonási eljárás fontosságára, mint kockázattal járó hiányosságra, de ezek megmaradnak az említés szintjén, és nem épülnek be átfogó modellbe vagy értelmezési keretbe.

A tudományos probléma tehát úgy foglalható össze, hogy hiányzik egy olyan átfogó fogalmi és empirikusan megalapozott keretrendszer, amely az IoT-alapú (különösen LoRaWAN-kommunikációra épülő) személy- és vagyonvédelmi rendszerek, végberendezések megbízhatóságát nem csak kommunikációtechnikai, de

biztonságtechnikai szempontból is értelmezi, figyelembe véve a teljes életciklus-menedzsmentet, beleértve annak lezárási szakaszát is. Mindezek hiányában az IoT alkalmazhatóságának értékelése személy- és vagyonvédelem szempontjából hiányos, és nem tükrözi a rendszerállapot és a kockázati vonulat teljes összefüggésrendszerét.

Az értekezés az alábbi kutatási kérdésekkel foglalkozik.

Szakirodalmi feldolgozásnál alapul vett kérdéseim:

- **Q1.1.** Hogyan definiálja a nemzetközi szakirodalom az IoT fogalmát, milyen rendszerszemléletű elemek találhatók meg a különböző megközelítésekben?
- **Q1.2.** Milyen kommunikációs sajátosságok jellemzőek az LPWAN IoT rendszerekben?
- **Q1.3.** A szakirodalom alapján milyen technikai és architekturális különbségek azonosíthatók a Sigfox, az NB-IoT és a LoRaWAN kommunikációk között, különös tekintettel a biztonsági és megbízhatósági jellemzőkre?
- **Q1.4.** Milyen korlátok, hiányosságok azonosíthatók a LoRaWAN technológiával kapcsolatban a vonatkozó specifikációk, technikai dokumentációk és tudományos publikációk alapján és milyen alkalmazási területeken tekintik relevánsnak a LoRaWAN technológiát?
- **Q1.5.** Milyen mértékben foglalkozik a szakirodalom a LoRaWAN technológia személy- és vagyonvédelmi kontextusú alkalmazhatóságával, és hogyan jelenik meg a biztonsági kockázat, a kulcskezelés, a rendelkezésre állás és az életciklus-menedzsment kérdésköre?

Tanúsított LoRaWAN eszközök elemzésére vonatkozó kérdéseim:

- **Q2.1.** Milyen dominanciák figyelhetők meg funkcionálisan a tanúsított LoRaWAN eszközök között és mi ezeknek a jelentősége személy- és vagyonvédelemben történő alkalmazhatóság vonatkozásában?
- **Q2.2.** Milyen szabványkövetési heterogenitás jellemzi a végberendezéseket és ennek milyen hatása van?
- **Q2.3.** A működési osztályok alakulása mennyiben korlátozza a valós idejű személy- és vagyonvédelmi alkalmazásokat?
- **Q2.4.** Kimutatható-e a folytonos életciklus-menedzsment megléte?

- **Q2.5.** A tanúsítás tényének megléte önmagában elegendő-e a biztonságtechnikai alkalmasság megítéléséhez?

Fogalmi keretrendszer kialakítását és megbízhatóság vizsgálatát megalapozó kérdéseim:

- **Q3.1.** Lehet-e értelmezni az IoT-alapú védelmi rendszert egységesen, ami több, mint a tisztán kommunikációs infrastruktúra-szemlélet?
- **Q3.2.** Meghatározható-e egy többdimenziós biztonságtechnikai modell a végpontok megbízhatóságára?
- **Q3.3.** Formalizálható-e a megbízhatósági modell a dimenziókra építve és azokat további paraméterekre bontva?
- **Q3.4.** Levezethető-e a megbízhatósági modellből a végpontok funkcionális kockázati besorolása?
- **Q3.5.** A kidolgozott modell alkalmas-e, hogy a végpontokat összehasonlítóan, rendszerszintű szemléletben értékelje?

A modellvalidációt és a méréseken alapuló megbízhatósági vizsgálatot megalapozó kérdéseim:

- **Q4.1.** A kommunikáció stabilitása és sikerességi rátája milyen mértékben függ a környezeti tényezőktől?
- **Q4.2.** A beállítási paraméterek változtatása milyen, nemlineáris hatást gyakorol a működési megbízhatóságra?
- **Q4.3.** A hálózati viselkedés megváltozása hogyan befolyásolja az észlelési és beavatkozási mechanizmusok hatékonyságát?
- **Q4.4.** A megbízhatósági dimenziók elkülöníthetők-e egymástól vagy kimutathatóak kölcsönhatások közöttük?
- **Q4.5.** A végpont életciklus-állapota milyen hatást gyakorol a rendszerre?

Az IoT-végpontok életciklus-menedzsmentjének lezárási szakaszát vizsgáló kérdéseim:

- **Q5.1.** Elegendő-e az IoT-végpont kivonására csupán üzemeltetési-adminisztratív műveletként tekinteni, ha az eszköz fizikai és logikai jelenléte szétválik?
- **Q5.2.** Milyen inkonzisztens állapot jöhet létre az eszköz logikai és fizikai szétválásakor és ennek nem megfelelő kezelése milyen következményekkel jár?

- **Q5.3.** Milyen rejtett védelmi kockázatot okoz, ha a végberendezés életciklus-lezárása nem történik meg formalizált módon, és ennek milyen torzító hatása van az állapotértékelésre?
- **Q5.4.** Milyen követelményeknek kell érvényesülnie egy IoT-végpont kivonása során, hogy az konzisztens, reprodukálható és auditálható legyen?
- **Q5.5.** Milyen lépésekben valósítható meg a LoRaWAN végberendezések kivonási eljárása és ez milyen összhangban van azok specifikációjával?

Célkitűzések

Az értekezés összetett célja a LoRaWAN-alapú IoT kommunikációs megoldások személy- és vagyonvédelmi alkalmazhatóságának rendszerszintű vizsgálata, a technológiai sajátosságok, a működési megbízhatóság és a biztonságtechnikai értelmezés összefüggéseinek aspektusában. A kutatás célja továbbá egy olyan mérésekkel alátámasztott keretrendszer kialakítása, amely megalapozza a LoRaWAN-alapú védelmi rendszerek alkalmazhatóságának, kockázatainak és életciklus-kezelésének tudományos igényű értékelését.

Ennek megfelelően a kutatás részletes célkitűzései az alábbiak:

- Áttekinteni a hazai- és nemzetközi szakirodalmat az IoT-alapú, személy- és vagyonvédelmi alkalmazásokhoz kapcsolódó kommunikációs technológiák vonatkozásában.
- Elemezni az IoT rendszerek sajátosságait rendszerszinten, különös tekintettel az érzékelőalapú, eseményvezérelt kommunikáció dominanciájára.
- Összehasonlító módon elemezni a nagy hatótávolságú, alacsony energiafogyasztású hálózatok (LPWAN) megoldásait, hangsúlyt helyezve a LoRaWAN, valamint a hasonló célú Sigfox és NB-IoT kommunikációkra.
- Megvizsgálni és azonosítani a LoRaWAN technológia korlátait, specifikációs hiányosságait és működési sajátosságait, kiemelt figyelemmel azok személy- és vagyonvédelmi jelentőségére.
- Behatárolni és értékelni a személy- és vagyonvédelmi alkalmazási területek releváns alrészeit, valamint meghatározni, hogy mely funkcionális környezetben tekinthető a LoRaWAN technológia reális alternatívának.

- Feltárni azokat a szakirodalmi és műszaki értelmezési hiányosságokat, amelyek indokolttá teszik a LoRaWAN technológia biztonságtechnikatudományi szemléletű vizsgálatát.
- Megvizsgálni és elemezni a tanúsított LoRaWAN végberendezések funkcionális felépítését, alkalmazási területeit, működési osztályait, specifikációs besorolását és frekvenciasáv-használatát, valamint összehasonlító elemzéssel értékelni két eltérő időpontban végzett nagymintás felmérés eredményeit a megjelenő mintázatok azonosításának érdekében.
- Kidolgozni és továbbfejleszteni egy funkcionális taxonómiát a tanúsított eszközök csoportosítására, a releváns kategóriák kijelölésével.
- Értékelni, hogy a tanúsítás megléte önmagában mennyiben tekinthető elegendőnek biztonságtechnikai alkalmassági feltételként.
- Kidolgozni és meghatározni az IoT-alapú elektronikai védelmi eszközök fogalmi- és modellkeretét, valamint elhatárolni a kommunikációs infrastruktúra-szintű és a biztonságtechnikai megbízhatósági értelmezését.
- Azonosítani és többdimenziós modellbe rendezni a megbízhatóságot befolyásoló tényezőket, valamint formalizálni azok értelmezési keretét.
- Kidolgozni egy kockázati osztályozási keretet, amely lehetővé teszi az IoT végpontok és rendszerek funkcionális összehasonlítását.
- Mérésekkel és kísérletekkel igazolni a többdimenziós megbízhatósági modell gyakorlati alkalmazhatóságát, valamint feltárni és értékelni a megbízhatósági dimenziók közötti kapcsolatokat.
- Igazolni, hogy a végpontok életciklus-állapota mérhető módon befolyásolja a rendszer megbízhatóságát és rejtett védelmi kockázatot eredményezhet.
- Rendszerszinten értelmezni az eszköz-életciklus szakaszait, különös tekintettel az életciklus lezárására.
- Kidolgozni és elvi megoldásként javasolni egy olyan életciklus-modellt és keretrendszert, amely biztosítja a következetes, ellenőrizhető és reprodukálható fizikai és logikai lezárást.

A téma kutatásának hipotézisei

A kutatáshoz az alábbi hipotéziseket (H1-H4) állítottam fel:

H1: Feltételezem, hogy a tanúsított LoRaWAN végpontok ökoszisztémájában empirikus vizsgálatok alapján azonosítható funkcionális dominancia, specifikációs heterogenitás és életciklus-dinamika olyan strukturális mintázatokat mutat, amelyek érdemben befolyásolják és differenciálják az alkalmazhatóságot, ezért az IoT-alapú személy- és vagyonvédelmi rendszerek nem értelmezhetők kizárólag kommunikációs infrastruktúraként.

H2: Feltételezem, hogy az IoT végpontok biztonságtechnikai értelemben vett megbízhatósága személy- és vagyonvédelmi környezetben nem írható le műszaki és kommunikációs paraméterek összességeként, hanem többdimenziós modellben formalizálható; a klasszikus „műszaki megbízhatóság” szemlélet önmagában nem elegendő a jellemzésére.

H3: Feltételezem, hogy a kidolgozásra kerülő megbízhatósági modell tényezői a LoRaWAN IoT végpontok személy- és vagyonvédelem szempontjából releváns működésére mérhető és kimutatható hatást gyakorolnak, valamint a modell alkotórészei között azonosítható kölcsönhatások jelentkeznek.

H4: Feltételezem, hogy az IoT-végpontok életciklus-lezárása, de különösen a hálózatból történő kivonásuk, a személy- és vagyonvédelmi rendszerek állapotát strukturálisan befolyásoló folyamat, amelyre konzisztens és auditálható kivonási eljárás kidolgozható; ennek hiányában rejtett védelmi kockázatok maradnak fenn, és a rendszer állapotértékelése torzult képet mutat.

Kutatási módszerek

Az értekezés kutatási módszertana többrétegű és integrált megközelítést alkalmaz, ötvözve az empirikus, logikai és (bizonyos mértékig) a matematikai módszereket. [12] Egyaránt alkalmaztam kvantitatív és kvalitatív elemeket is az elméletorientált és a gyakorlati alapú célok megvalósításához. A kutatási téma több ismeretterületet is érint, a biztonságtechnika mellett más tudományterületek vizsgálata is megjelenik. Ezért, a kutatási módszerek megválasztásánál kiemelt szempont volt a rendszerszemléletű, a szükséges mértékű teljességre törekvő megközelítés. Cél volt, hogy ne csak elméleti feldolgozás jelenjem meg az értekezésben, hanem empirikus eredményekkel

alátámasztható, validálható következtetések is. Az értekezés a szakirodalmi és dokumentációs háttér feldolgozásából indul ki, de támaszkodik saját adatfeldolgozásra, mérésekre és ezek statisztikai értékelésére is.

A kutatómunka megalapozásához irodalmi feldolgozást végeztem, ahol első lépésben a tématerület feltérképezése és az alapinformációk rendszerezése jelent meg célként. Kezdeti lépés volt az IoT, LoRaWAN technológia és a személy- és vagyonvédelmi alkalmazási környezetek kapcsolódó tématerületeinek összegzése és rendszerezése. Rendszereztem az IoT-hoz kapcsolódó alapfogalmakat, architekturális elemeket és működési mechanizmusokat. Emellett, behatároltam az LPWAN személy- és vagyonvédelem területén való alkalmazásának releváns részterületeit. Ezekhez elérhető hazai és nemzetközi publikációkat, tanulmányokat, valamint specifikációkat, technikai dokumentációkat, ajánlásokat, szabványokat dolgoztam fel. A fogalmak, mechanizmusok és korlátok megismeréséhez analízist alkalmaztam. A technológiai részleteket összehasonlítással vizsgáltam. Az elemek rendszerszintű értelmezése szintézis alapú volt. Az irodalmi feldolgozás célja az volt, hogy azonosítsa a kutatási réseket és a vizsgálandó strukturális hiányosságokat, előkészítve az értekezés 2-5. fejezeteit.

A kutatás empirikus kiindulópontját a tanúsított LoRaWAN eszközök nagy elemszámú strukturált feldolgozása jelentette, ahol kvantitatív módszerekkel elemeztem többek között a végberendezések funkcionális dominanciáját, specifikációkövetési heterogenitást, működési osztályok arányát, életciklus-menedzsment megjelenését és kapcsolatot a személy- és vagyonvédelemmel. A módszer célja olyan mintázatok kimutatása volt, amelyek megalapozzák a 3. fejezet fogalmi és dimenzionális modelljét, valamint előkészítik a 4. fejezet validációra vonatkozó méréseit.

Az 1. fejezetben azonosított irodalmi hiányosságokra és a 2. fejezet empirikus vizsgálatának eredményeire építve logikai módszerek alkalmazásával kidolgoztam az IoT végpontok biztonságtechnikai aspektusban értelmezhető megbízhatóságát és többdimenziós modelljét. Elválasztottam a kommunikációs működőképességet a személy- és vagyonvédelemben értelmezhető megbízhatóságtól, dimenziómodellt és fogalmakat definiáltam, ezekből mérhető következményeket vezettem le és egységes keretrendszerbe illesztést valósítottam meg.

Az elméleti eredmények (fogalmak, dimenziók, keretrendszer) ellenőrzésére mérés és kísérlet alapú validációt végeztem. Vizsgáltam a paramétermanipuláció hatását és azok

kompromisszumos jellegét. Méréseket végeztem a környezeti változók és a dimenziók értelmezésére. A mérési és kísérleti eredmények feldolgozásával és statisztikai értékelésével kölcsönhatásokat azonosítottam, kimutattam a dimenziók közötti összefügéseket.

A kutatás záró szakaszában a végpontok életciklus-menedzsmentjét és életciklusának lezárását, illetve a LoRaWAN specifikációkban nem formalizált kivonási problémát vizsgáltam, amely specifikáció- és követelményelemzésre, logikai állapotmodellezésre, valamint eljárás- és követelményrendszer kidolgozására épült.

A kutatás folyamata és a doktori értekezés felépítése

A kutatás előre meghatározott koncepcionális keretben indult 2019-ben, amelynek középpontjában a LoRaWAN-alapú végberendezések személy- és vagyonvédelem területén történű alkalmazhatósága állt. A vizsgálat nemlineáris, nem egyirányú folyamatként valósult meg, hanem fokozatosan építkező, de visszacsatoló szakaszok összeségeként. Ezen eredmények logikai összegzései folyamatosan járultak hozzá az értekezés végső szerkezeti felépítéséhez.

Az értekezés kiindulópontja annak a problémának azonosítása volt, hogy eltérő nézőpont szükséges az IoT rendszerek személy- és vagyonvédelemben történő alkalmazása tekintetében összehasonlítva a hétköznapi megoldásokkal, azaz az értekezés nem csupán egy irodalmi áttekintésre építkezik, hanem alkalmazásorientált, rendszerszintű vizsgálatra. Az erre irányuló kutatási szakasz az 1. fejezetben jelenik meg. Az empirikus vizsgálatok két időpontban történtek 2020-ban és 2024-ben a tanúsított LoRaWAN végpontok strukturális elemzésének céljából. A feltárt empirikus mintázatokat és eredményeket a 2. fejezet foglalja össze. A többdimenziós modell kidolgozását folyamatosan, a feltárt hiányosságok, empirikus tapasztalatok és mérési eredmények szintéziseként valósítottam meg a 3. fejezetben ismertetettek mentén. A méréseket folyamatosan végeztem 2019-2025 között, melyek eredményeit felhasználtam a modellalkotásra és annak validációjára, további összefüggések megállapítására. A 4. fejezet foglalja össze az értekezés szempontjából releváns méréseket és azok értékelését. A kutatás folyamata során többször megjelent az életciklus-menedzsment kérdésköre és a megfelelő életciklus-lezárás hiánya, ennek megoldására dolgoztam ki az 5. fejezetben ismertetett módszert.

Alaki és formai megjelenés

Az értekezésben felhasznált szakirodalmi forrásokra történő hivatkozások a törzsszövegben, az Óbudai Egyetem Biztonságtudományi Doktori Iskola formai előírásainak megfelelően, szögletes zárójelben „[ ]” feltüntetett, sorszámozott jelöléssel szerepelnek. A hivatkozások részletes bibliográfiai adatai az értekezés végén, az Irodalomjegyzék fejezetben kerülnek rendszerezésre az előfordulás sorrendjében. Az értekezésben szereplő ábrák és táblázatok külön jegyzékben, az Ábrajegyzék és Táblázatjegyzék részek alatt találhatók, forrásmegjelöléssel ellátva. Az ábrák és táblázatok eltérő jelölés hiányában a szerző saját kutatási eredményeit tartalmazzák. A szövegben alkalmazott rövidítések és betűszók összegyűjtve, ábécérendben, a Rövidítésjegyzék fejezetben kerülnek felsorolásra. A szöveghez kapcsolódó kiegészítő megjegyzések számozott lábjegyzetek formájában jelennek meg.

Az értekezés jelen felépítése a kutatás természetes fejlődését tükrözi, amely 2026.03.02-án zárult.

1 IOT TECHNOLÓGIÁK A SZEMÉLY- ÉS VAGYONVÉDELEMBEN

Jelen fejezet célja egy olyan hazai- és nemzetközi szakirodalmi áttekintés, amely vizsgálja az értekezés szempontjából releváns, a személy- és vagyonvédelmi alkalmazásokhoz kapcsolódó IoT (Internet of Things – Dolgok Internete) technológiákat. A fejezet összefoglalja az IoT rendszerek kialakítási és működési jellemzőit, ismerteti a nagy hatótávolságú, alacsony energiafogyasztású hálózatok (LPWAN - Low Power Wide Area Network) kommunikációs megoldásait. A fő fókusz a LoRaWAN jellemzőin van, de megjelennek hasonló célú megoldások is, mint a Sigfox és a NB-IoT rendszerek is.

A szakirodalmi feldolgozást a következő kérdések mentén végeztem:

- Hogyan definiálja a nemzetközi szakirodalom az IoT fogalmát, milyen rendszerszemléletű elemek találhatók meg a különböző megközelítésekben? (Q1.1.)
- Milyen kommunikációs sajátosságok jellemzőek az LPWAN IoT rendszerekben? (Q1.2.)
- A szakirodalom alapján milyen technikai és architekturális különbségek azonosíthatók a Sigfox, az NB-IoT és a LoRaWAN kommunikációk között, különös tekintettel a biztonsági és megbízhatósági jellemzőkre? (Q1.3.)
- Milyen korlátok, hiányosságok azonosíthatók a LoRaWAN technológiával kapcsolatban a vonatkozó specifikációk, technikai dokumentációk és tudományos publikációk alapján és milyen alkalmazási területeken tekintik relevánsnak a LoRaWAN technológiát? (Q1.4.)
- Milyen mértékben foglalkozik a szakirodalom a LoRaWAN technológia személy- és vagyonvédelmi kontextusú alkalmazhatóságával, és hogyan jelenik meg a biztonsági kockázat, a kulcskezelés, a rendelkezésre állás és az életciklus-menedzsment kérdésköre? (Q1.5.)

Az áttekintés célja elsődlegesen nem a különböző technológiák ismertetése, hanem az értekezés 2-5. fejezeteinek megalapozása és annak a bemutatása, hogy a működési sajátosságok hogyan hatnak és jelennek meg a személy- és vagyonvédelmi rendszerek tervezésekor, működésekor és milyen korlátot jelentenek az alkalmazhatóság aspektusában. A fejezet célja azonosítani azokat a szakirodalmi hiányosságokat, amelyek

indokolttá teszik a téma biztonságtechnikatudományi szemléletű vizsgálatát. Ezzel megteremtve az értekezés fejezeteiben ismertetett empirikus elemzések, modellalkotási lépések és rendszerszintű értelmezések technológiai és elméleti alapját, biztosítva a kutatás koherens tudományos keretét.

1.1 IoT fogalma és rendszerszemlélete

Az IoT körét tekinthetjük az információs és kommunikációs technológiák (ICT - Information and Communications Technology) egyik legdinamikusabban növekvő területének, hiszen a műszaki körökben a mindennapi munka része és számos tudományos publikáció központi eleme. [13] Ugyanakkor az IoT fogalmi értelmezése a különböző szakirodalmakban eltérő módon jelenik meg, nem egységes. [14][15][16][17][18][19] Bár a megfogalmazások nem azonosak, de számos közös elem megtalálható bennük. Ezeket összefoglalva, az IoT fogalmát a következő módon fogalmaznám meg [20]: Az IoT olyan beágyazott technológiákat alkalmazó fizikai eszközökből álló elosztott hálózatként értelmezhető, amelyek egymással kommunikálnak, saját állapotukat felügyelik, valamint adatokat továbbítanak egy magasabb szintű, integrált informatikai rendszernek. Az IoT rendszerek kialakulását, fejlődését és elterjedését a rádiófrekvenciás azonosítás (RFID - Radio Frequency IDentification) térhódításával azonosítják [18], amely már lehetővé tette a fizikai eszközök hálózatba integrálását.

A statisztikai trendeket megvizsgálva, alátámasztott az IoT globális növekedése. [21][22] A világban működő IoT-eszközök száma 2024-ben megközelítőleg 18,6 milliárd volt, de az előrejelzések szerint 2030-ra ez akár 39 milliárd is lehet, ami éves szinten 10-14%-os emelkedést vetít előre. [23] Egy másik elemzés szerint az IoT-kapcsolatok száma 2030-ra 38,7 milliárd nagyságrendre tehető, amely a technológia folyamatos emelkedő terjedését jelzi világszerte. [21] Egyéb piaci elemzések azt prognosztizálják, hogy az IoT-piac nagysága a 2025-ös 1,35 billió dollárról 2030-ra 2,72 billiárd dollárra növekszik, azaz megduplázódik. [24]

Nemzetközi szabványosítási törekvések is elindultak [25][26][27], melyek többrétegű, elosztott architektúraként írják le az IoT rendszereket. Az ISO/IEC 30141 referenciaarchitektúrában [28] elkülönül az eszközréteg, hálózati réteg, adatfeldolgozó réteg, valamint az alkalmazási réteg [29]. Továbbá elválasztja a menedzsment- és biztonsági funkciókat. [28] Az egyes IoT rendszerek eltérő műszaki adottságokkal, más

kommunikációs képességekkel és energiaellátási profillal rendelkeznek. Ez a sokszínűség és rugalmasság integrációs kihívásokat eredményez és növeli a komplexitást. A végpontok gyakran korlátozottak erőforrásukban, ami befolyásolja a kommunikációs stratégiát, ezzel egyben az adatküldési időbeliséget is.

A személy- és vagyonvédelem területén alkalmazott IoT megoldásoknak megvannak a maga kompromisszumai. Olyan területekben kell gondolkozni, ahol a végpontok elsődleges feladata a vonatkozó állapotok érzékelése és jelzése, nem nagymennyiségű adatok folyamatos továbbítása. Ezért elengedhetetlen az IoT rendszerek kommunikációs megoldásainak olyan nézőpontú vizsgálata, hogy azok milyen mértékben és milyen kompromisszumok mellett képesek támogatni a védelmi[1] feladatokat.

Összességében az IoT olyan elosztott, rétegzett és heterogén infrastruktúrát jelent, amelyben a fizikai környezet érzékelése, a kommunikáció és a támogató feldolgozás együttműködő módon valósul meg. A továbbiakban ismertetett LPWAN technológiák, valamint azok személy- és vagyonvédelmi alkalmazási lehetőségeinek vizsgálata ezt a rendszerszintű szemléletet veszi alapul.

1.2 LPWAN technológiák

Az IoT rendszerekben alkalmazott különböző kommunikációs megoldások széles spektrumot fednek le egészen a rövid hatótávolságú, nagy adatsebességű technológiáktól (Wi-Fi [30], Bluetooth Low Energy [31], Zigbee [32]), a mobilhálózati megoldásokon keresztül (NB-IoT [33], LTE-M [34], 5G [35]) egészen a műholdas infrastruktúrákig (Iridium [36], Swarm [37], Sateliot [38]). Az LPWAN kommunikációk alapvetően eltérnek a klasszikus IP[2]-alapú, folyamatos adattovábbításra optimalizált hálózati megoldásoktól. Az LPWAN megoldások egyik fő szempontja az energiahatékonyság, a másik pedig a nagy hatótávolság [39], ahogy azt az elnevezés is mutatja. Ez a különbség közvetlen hatást gyakorol a személy- és vagyonvédelmi alkalmazhatóságra.

Az LPWAN rendszerek olyan alkalmazásokat szolgálnak ki, amelyek alacsony adatforgalommal járnak, főként elemes tápellátást igényelnek, nagy kiterjedésű területeket ölelnek fel és nem igényelnek folyamatos kapcsolatot. [40] Jellemzően alkalmazásuk kompromisszumokkal jár az energiafogyasztás [41], adatsebesség és kommunikációs rendelkezésre állás hármasával. Különösen alkalmasak olyan

[1] Az értekezés a személy- és vagyonvédelemre védelem összefoglaló szóval is hivatkozik.
[2] IP: Internet Protocol – Internetprotokoll.

megoldásokban, amik valami szenzorhálózatra épülnek, állapotfelügyeletet valósítanak meg és eseményvezérelten működnek. Három piacot uraló [42] LPWAN kommunikációt vizsgálok és hasonlítok össze ebben az alfejezetben: Sigfox, NB-IoT, LoRaWAN. A LoRaWAN kommunikációval részletesebben a következő alfejezet fog foglalkozni. Az 1. táblázat foglalja össze a három LPWAN kommunikáció releváns tulajdonságait.

Szempont	**Sigfox**	**NB-IoT**	**LoRaWAN**
LPWAN piac	~6%	~44%	~41%
Frekvenciasáv (Európa)	868 MHz (nem licencelt, ISM)	LTE[3] licencelt	868 (433) MHz (nem licencelt, ISM)
Topológia	Csillag	Cellás	Összetett csillag
Energiafogyasztás	Nagyon alacsony (10+ év)	Közepes (3-7 év)	Alacsony (5-10 év)
Sávszélesség	100 kHz	200 kHz	125 kHz, 250 kHz
Adatátviteli sebesség	100 bit/s	250 kbit/s	50 kbit/s (adaptív)
Adatirány	Erősen korlátozott	Kétirányú	Részben korlátozott
Üzenetszám-korlátozás	Napi limit	Nincs fix limit	Duty-cycle limit
Hasznos adat (maximum)	12 byte Erősen korlátozott	1600 byte Nagyobb	222 byte Korlátozott, de rugalmas
Interferencia immunitás	Nagyon magas	Licencelt spektrum – nem releváns	Nagyon magas
Adatátviteli távolság (maximum)	50 km	10 km	15 km
Titkosítás, hitelesítés	Nem implementált	Implementált (LTE)	Implementált (AES128)
Hálózati kontroll	Alacsony	Alacsony	Magas (privát hálózat lehetősége)
Telepítési rugalmasság	Korlátozott	Szolgáltatófüggő	Magas
Függetlenség külső szolgáltatótól	Nem	Nem	Lehetséges
Modul ára	~2$	~5$	~10$
Gateway ára	5000$	15000$	100-2000$
Frekvenciaszolgáltatás ára	Ingyenes	>500$ millió (szolgáltató költsége)	Ingyenes
Költségstruktúra	Előfizetés-alapú	Előfizetés + SIM	Infrastrukturális beruházás + alacsony üzemeltetés
Kommunikáció determinisztikusága	Nem garantált	Beépített QoS	Nem garantált
Jellemző késleltetés	~1 s	<1 s	~1-2 s
Kritikus riasztási alkalmasság	Korlátozott	Megfelelő	Tervezési kompromisszumokkal
Felügyeleti/Állapotjelző alkalmasság	Alkalmas	Alkalmas	Kifejezetten alkalmas

1. táblázat - Sigfox, NB-IoT, LoRaWAN összehasonlítása [41][43][44][45] [46][47][48][49]

[3] LTE: Long Term Evolution - Hosszú távú evolúciójú mobilhálózati technológia.

A három közül a legalacsonyabb piaci részesedéssel bíró kommunikáció a ***Sigfox***, amely egy ultra-keskenysávú, 868 MHz-es ISM (Industrial, Scientific and Medical: Ipari, tudományos és orvosi) sávban működő LPWAN kommunikáció. A hálózati kialakítása csillag topológiára épül és rendkívül alacsony fogyasztásának köszönhetően akár 10 évig is képes működni beavatkozás nélkül. A megoldás egyik nagy erőssége a több tíz kilométeres adatátviteli távolság és a kiemelkedő interferencia immunitás, de adatátviteli sebessége, a hasznos adat hossza és a napi üzenetszám jelentősen korlátozott. Kialakítása szolgáltatói infrastruktúrát igényel, ami befolyásolja a hálózati kontrollt és a telepítési rugalmasságot. Személy- és vagyonvédelmi alkalmazásokban a Sigfox elsősorban nem időkritikus, alacsony adatforgalmú, kifejezetten állapotjelző megoldásokban lehet egy jó választás. Kritikus riasztási funkciók esetén a korlátozott kétirányú adatforgalom és az üzenetlimit tervezési korlátként jelenik meg.

A LoRaWAN és a NB-IoT közel azonos nagyságrendben uralja az LPWAN IoT piacot. Az ***NB-IoT*** celluláris topológiára épülő kommunikáció, melyet a 3GPP[4] [50] szabványosított és több biztonsági, hitelesítési és szolgáltatásminőség (QoS - Quality of Service) mechanizmust implementál. A versenytársakhoz képest az adatátviteli sebessége lényegesen nagyobb és a továbbítható hasznos adat mérete, az 1600 bájttal, kategóriájában kiemelkedő. A kommunikáció kétirányú és nem korlátozott, viszont a rendszer teljes mértékben függ szolgáltatótól. [43] Az alkalmazott eszközök ára és a folyamatos szolgáltatási költségek a drágább megoldások közé sorolják. Személy- és vagyonvédelmi rendszerekben történő alkalmazás szempontjából előnyös kommunikációs és időzítési tulajdonságokkal rendelkezik, de a teljes operátori függőség stratégiai kockázatként megjelenik.

A ***LoRaWAN*** kommunikáció nem licencelt ISM sávban működik, hálózati topológiája összetett csillag (star-of-stars). Adatátviteli sebessége relatív alacsonynak mondható, viszont képes azt adaptívan (ADR - Adaptive Data Rate) [48] változtatni. Az energiafogyasztás alacsony (5–10 év tipikus élettartam), a hasznos adat hossza alkalmazás függvényében módosítható (akár 222 byte), amely továbbítása során AES-128 alapú hitelesítési modellt használ. A kommunikáció nem determinisztikus, korlátozás alá esik az ingyenes ISM frekvencia vonatkozó szabályai alapján. A LoRaWAN egyik legfontosabb jellemzője, hogy privát hálózatként is megvalósítható, így biztosítható a

[4] 3GPP: 3rd Generation Partnership Project – Harmadik Generációs Partnerségi Projekt.

teljes hálózati felügyelet és külső szolgáltatótól való függetlenség érhető el. Személy- és vagyonvédelmi alkalmazásban a LoRaWAN különösen megfelelő felügyeleti és állapotjelző rendszerekben, valamint ott, ahol az infrastruktúra saját kézben tartása stratégiai jelentőségű. Ugyanakkor meg kell említeni, hogy időkritikus riasztási funkciók megvalósítása tervezési kompromisszumokat igényel.

Az előző összehasonlítás alapján jól látszik, hogy az LPWAN technológiák különböző szempontok szerint optimalizáltak és eltérő tulajdonságokkal rendelkeznek. A Sigfox jelentősen alacsony energiaigényű, de kommunikációs tekintetben rendkívül korlátozott, ezért elsősorban egyszerű, ritka adatküldést igénylő alkalmazások esetén javasolt. A NB-IoT kedvezőbb, stabilabb, nagyobb kapacitású kommunikációs feltételeket biztosít, de erősen szolgáltatófüggő a kialakítása és a költsége is. A LoRaWAN, az összehasonlító elemzés alapján, e két technológiai megközelítés között helyezkedik el. Bár kommunikációs szempontból az NB-IoT-hoz képest kompromisszumos megoldást kínál, ugyanakkor a Sigfox-szal összehasonlítva több kedvezőbb paraméterrel is rendelkezik és a privát hálózat kialakításának opciója lehetőséget biztosít az infrastruktúra feletti teljes kontrollra, amely a személy- és vagyonvédelmi rendszerek esetében egy döntő szempont lehet.

Mindezek figyelembevételével, az értekezés vizsgálati és kiindulási alapnak a LoRaWAN-t tekinti, mint az LPWAN kommunikációk jellemzőinek végletei közötti, gyakorlati szempontból is jól implementálható megoldást.

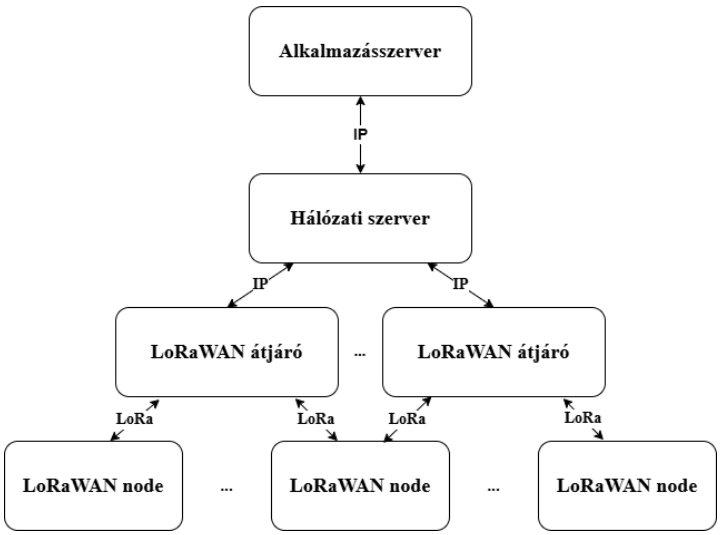
1.3 LoRaWAN technológia jellemzői

A LoRaWAN technológia a LoRa (Long-Range) kommunikáció fizikai rétegre épülő, alacsony energiafogyasztású, nagy hatótávolságú vezetéknélküli megoldás, amelyet kifejezetten IoT rendszerekhez optimalizáltak. A kommunikáció specifikációján és továbbfejlesztésén 2015 óta a LoRa Alliance [51][52] dolgozik, emellett a megfelelési tanúsításért is ők felelősek. A szervezet által kidolgozott specifikációk – v1.0 (2015) [48], v1.0.1 (2016) [53], v1.0.2 (2016) [54], v1.0.3 (2018) [55], v1.0.4 (2020) [56] és v1.1 (2017) [57] – egymásra épülve folyamatos fejlesztéseken estek keresztül. Az 1.0.x klasszikus verziók az előző változatok hibajavításait, pontosításait tartalmazták úgy, hogy visszafelé kompatibilisek maradtak egymással. A specifikációk jelentőségét a 2. fejezet tartalmazza részletesebben. A specifikációk és a kapcsolódó dokumentumok nagy nyitva hagyott kérdése a hálózatból történő eszközkivonás (exit procedure) [58][56][59][60]

formalizált kezelése. Erre a kapcsolódó publikációkban sem jelenik meg megoldás. [61][62][63]

A LoRaWAN hálózati modellje alapvetően más, mint a cellás vagy lokális hálózatok felépítése. A klasszikus LoRaWAN architektúra (1.0.x) [54] négy fő komponensből áll star-of-stars topológiában, ahogy azt az 1. ábra is mutatja:

- végberendezések (végpont, node, end-node),
- átjárók (gateway).
- hálózati szerver,
- alkalmazásszerver.



1. ábra - LoRaWAN hálózati felépítése

A végberendezések és a gateway-ek között LoRa rádiós interfészen [54] keresztül valósul meg a kommunikáció. A hálózaton belül az átjárókból is lehet több, így egy végberendezés üzeneteit, akár több is fogadhatja, ezzel növelhető a lefedettség, redundancia és robusztusság. A végberendezések egymás között közvetlenül nem tudnak kommunikációt megvalósítani. A gateway-ek valamilyen IP-alapú hálózaton továbbítják a hálózati szerver felé az üzeneteket. A hálózati szerverek látják el a hálózatmenedzsment funkcióját, kezelik a csomag-duplikációt, kulcsokat, azonosítókat, ellenőrzik az üzenetek hitelességét, menedzselik az eszközöket. [64] Az alkalmazásszerverek végzik az adatok dekódolását és esetlegesen a feldolgozását, ide illeszthetők a megjelenítő- és felhasználói felületek. Az 1.1-es specifikációban megjelenik az architektúra kiterjesztése és a kulcskezelési folyamat átdolgozása, ezzel együtt egy új hálózati elem a Join Server is. [57]

A hálózati résztvevőknek eltérő biztonsági kihívásokkal kell szembenézniük. A végberendezések vannak a leginkább kitéve fizikai jellegű hatásoknak, mivel legtöbbször kültéri vagy nyilvánosan hozzáférhető helyre kerülnek telepítésre. Itt nem csak a szándékos manipulációra kell gondolni, hanem a környezeti hatások is erőteljesek. A LoRaWAN végberendezések többsége telepes üzemű, ezért a megfelelő tervezés és a folyamatos monitorozás elengedhetetlen. Itt ki kell még emelni a nem megfelelő antennakialakítást [64][65] vagy elhelyezést, hiszen a gyakorlatban sokszor ez okozza a kommunikáció instabilitását. Az antenna mellet kiemelten fontos az optimális rádiós paraméterek megválasztása a megfelelő kommunikációs kapcsolat kialakításához és fenntartásához. A gateway-ek a hálózat kritikus elemei [66], mivel kiesésük lokális kommunikációs megszakadást okozhat, amennyiben nem áll rendelkezésre redundáns lefedettség.

Rádiós szempontból a LoRa fizikai réteg a jelentős, amely egy speciális, úgynevezett Chirp Spread Spectrum[5] (CSS) modulációt alkalmaz [67]. Ez a modulációs eljárás teszi lehetővé azt, hogy elérhetővé váljon a nagy hatótávolság, a kiemelkedően magas interferencia immunitás és a sikeres adatátvitel alacsony jel-zaj viszony mellett is. Európában (EU) a kommunikáció jellemzően a 863-870 MHz-es ISM sávban történik, tipikusan 868 MHz és környéke, de engedélyezett a 433 MHz-es sáv is. [68] A frekvenciák használata bár ingyenes, de korlátokhoz kötött. A kommunikáció az idő 1%-át töltheti ki (duty cycle) [68], de vannak ennél szigorúbb korlátozások is. Az adatátviteli sebesség a terjedési tényező (SF – Spreading Factor) és a sávszélesség függvénye (BW – Bandwidth), 0,3-50 kbit/s tartományban mozog. Egyszerűen szokták jellemezni a mesterségesen létrehozott adatráta (DR – Data Rate) számmal is a kommunikációt. A nagyobb DR érték (kisebb SF) nagyobb adatátviteli sebességet jelent, de kisebb hatótávolságot, ahogy a 2. táblázat is mutatja.

DR index	**Moduláció**	**SF**	**BW [kHz]**	**CR[6] (tipikus)**	**Sebesség [bit/s]**
DR0	LoRa	SF12	125	4/5	~290
DR1	LoRa	SF11	125	4/5	~440
DR2	LoRa	SF10	125	4/5	~980
DR3	LoRa	SF9	125	4/5	~1760
DR4	LoRa	SF8	125	4/5	~3125
DR5	LoRa	SF7	125	4/5	~5470

2. táblázat - LoRaWAN rádiós paraméterek [54][69][70]

[5] CSS (Chirp Spread Spectrum): chirp jelformákon alapuló szórt spektrumú modulációs eljárás.
[6] CR: Coding Rate - Kódolási ráta. Tipikus értéke 4/5.

A kommunikáció alapvetően kétirányú, de jellemzően a végpont → hálózati szerver irány a domináns. Az üzenetek kétfajták lehetnek irányuk szerint:

- downlink: hálózati szerver → végpont,
- uplink: végpont → hálózat szerver:
    - confirmed: nyugtázott,
    - unconfirmed: nyugtázás nélküli. [54]

Az uplink üzenetek esetén kérhető nyugtázás a hálózati szervertől sikeres beérkezéskor, ellenkező esetben nincs visszajelzés. A kommunikáció aszinkron módon folyik ALOHA-alapú csatornahozzáféréssel, nem garantálva a determinisztikus működést; különösen nagy végpontszám esetén ütközések előfordulhatnak.

A LoRaWAN három végpont-működési osztályt [56] határoz meg, ahol a különbség a rendelkezésre állásban, a vételi ablakban van:

- Class A (A osztály): alacsony energiafogyasztásra optimalizált működés, küldés után érhető el két rövid vételi ablak a fogadáshoz;
- Class B (B osztály): az uplink-ek között periodikusan, ütemezetten érhetőek el vételi ablakok;
- Class C (C osztály): küldések között folyamatosan képes vételre, ezzel nagyobb energiafogyasztást eredményezve.

Látható, hogy a downlink irányú kommunikáció vételi ablakhoz van kötve [71] különösen az A osztályú működés esetén.

A LoRaWAN AES-128 alapú titkosítást alkalmaz, ami miatt a kommunikáció során több azonosító és kulcs is felhasználásra kerül. Ezt foglalja össze a 3. táblázat, melyben megkülönböztetésre kerülnek a csatlakozás előtt és után tárolt kulcsok és azonosítók. A végberendezések hálózathoz történő csatlakozása kétféle módon történhet:

- Activation by Personalization (ABP) – előre letárolt, statikus kulcskezelés;
- Over-the-Air Activation (OTAA) – dinamikus kulcscsere a kommunikáció során, handshake-alapú folyamat. [54]

Az azonosítók és kulcsok egy része a végberendezésen és a szervereken is tárolásra kerül, melyek biztonságos kezelése alapkövetelménynek tekinthető rendszertervezés és az üzemeltetés során. Az ABP statikus kulcskezelést használ, változó kulcsok nélkül, ami csökkentett szintet eredményez, ezért csak fejlesztési, tesztelési szakaszban javasolt az

alkalmazása. Ezzel szemben, az OTAA dinamikus kulcskezelés miatt magasabb védelmi szintet jelent, valós alkalmazásokban használata erősen ajánlott.

Specifikáció	ABP előtt	ABP után	OTAA előtt	OTAA után
1.0 **1.0.1** **1.0.2** **1.0.3**	DevAddr NwkSKey AppSKey	DevAddr NwkSKey AppSKey	DevEUI AppEUI AppKey	AppEUI DevEUI AppKey NwkSKey AppSKey
1.0.4	DevAddr NwkSKey AppSKey	DevAddr NwkSKey AppSKey	DevEUI JoinEUI AppKey	AppEUI DevEUI AppKey NwkSKey AppSKey
1.1	DevAddr FNwkSIntKey SNwkSIntKey NwkSEncKey AppSKey	DevAddr FNwkSIntKey SNwkSIntKey NwkSEncKey AppSKey	DevEUI JoinEUI AppKey NwkKey	JoinEUI AppKey NwkKey FNwkSIntKey SNwkSIntKey NwkSEncKey AppSKey

3. táblázat - ABP és OTAA kulcsok és azonosítók[7] (Készítette a szerző: [72])

További beépített mechanizmus a korábban rögzített és újraküldött üzenetek elleni védelem biztosítása. Ennek alapja a keretszámláló (FCnt - frame counter) integrálása, amely minden uplink és downlink üzenethez növekvő számlálóértéket rendel. [54] Csak az az üzenet tekinthető érvényesnek, amelynek keretszámláló értéke nagyobb a korábban rögzítettnél, így egy lehallgatott és később ismételten továbbított csomagot automatikusan el lehet utasítani. Az ABP és OTAA csatlakozási módokban eltérően történik a keretszámlálók menedzselése, de mindkét esetben következetesen le kell kezelni a számláló túlcsordulását, különben kommunikációs anomália lép fel. [54] A keretszámláló más területeken is hasznosnak bizonyul, amiről az értekezés 4. fejezetében lesz szó.

A LoRaWAN kommunikációs és specifikációs alapjellemzőit figyelembe véve több megállapítás is összefoglalható:

- a gateway-ek szerepe viszonylag passzív, ezért a hálózatmenedzsment szerverközpontú,
- az ISM sáv használata bár ingyenes, de nem garantálja a prioritást,

[7] A táblázatban szereplő azonosítók és kulcsok értelmezése a Rövidítésjegyzékben található. Az *Addr* és *EUI* végződések azonosítókra utalnak; a *Key* végződések pedig hitelesítési és titkosítási kulcsokra.

- a duty-cycle korlátozás és az uplink üzenetközpontúság hatással van az időkritikus alkalmazásokra,
- a nem determinisztikus csatornahozzáférés befolyásolja a késleltetést [73],
- a privát hálózat lehetősége teljes üzemeltetési kontrollt biztosít.

Az ismertetett hálózati és kommunikációs jellemzők alapján megállapítható, hogy bár a LoRaWAN tervezési szempontból kellő rugalmasságot kínál, de személy- és vagyonvédelem területén történő alkalmazás szempontjából több korlátot [74] is hordoz magában.

A megvizsgált szakirodalom és technikai dokumentumok alapján nincs egy egységes módszer, hogy miként kezelendők a kulcsok és azonosítók, ha a végberendezést véglegesen eltávolítják egy rendszerből. A kutatások legnagyobb része a LoRaWAN technológia rádiós teljesítményére, lefedettségére és energiahatékonyságára fókuszál, miközben az alkalmazási következmények, az eltérő környezetben jelentkező kockázatok és az életciklus-menedzsment kérdései kevésbé kerülnek elemzésre.

A feltárt működési sajátosságok és szakirodalmi hiányosságok indokolják a technológia alkalmazási kontextusba ágyazott vizsgálatát, különösen a személy- és vagyonvédelmi rendszerek területén, ahol az időbeliség, a rendelkezésre állás és a megbízhatóság nem egyszerűsíthető le műszaki paraméterekre, hanem közvetlen jelentőséggel bír.

1.4 A LoRaWAN alkalmazhatóságának behatárolása a személy- és vagyonvédelem területén

A személy- és vagyonvédelem területe elég nagy és szerteágazó, ezért fontos behatárolni, hogy mely részegységek érintettek IoT, de kifejezetten LoRaWAN szempontjából. A vagyonvédelem meghatározó része az elektronikus vagyonvédelem, ezen belül is kiemelhetők az elektronikus jelzőrendszerek relevancia tekintetében. A szakirodalom eltérő csoportosításokat alkalmaz az elektronikus vagyonvédelem alrendszereire, melyek közül a következő felosztás szolgál kiindulópontként: kültéri védelem, behatolásjelző rendszerek, beléptető rendszerek, távfelügyeleti rendszerek, kamerás megfigyelőrendszerek (CCTV - Closed Circuit Television), áruvédelmi rendszerek. [75][76]

Mivel a LoRaWAN alacsony adatsebességen, maximum 50 kbit/s (régió és paraméterfüggő), működik és korlátozott a továbbítható adatok száma, maximum 222

byte (de a gyakorlatban többnyire néhány vagy néhány 10 byte), ezért nem alkalmas nagy sávszélesség-igényű adatfolyamok, így folyamatos videó- vagy hangátvitel megvalósítására. Ezért első körben a CCTV rendszerek, melyek alapvetően nagymennyiségű képi információ továbbítására épülnek [77], a vizsgálatból kizárhatók.

Az elektronikus kültéri védelem eszközei és a behatolásjelző rendszerek esetében már más a helyzet. Ezen csoportok eszközei jellemzően érzékelők, amelyek vagy eseményvezérelt vagy periodikus jelzéseket továbbítanak egy központi- vagy feldolgozóegység felé. [75] A jelzések analóg vagy digitális jellegűek lehetnek, de LoRaWAN szempontjából nem a fizikai mért mennyiség a meghatározó, hanem az információtovábbítás jellege. Ha az érzékelő kisméretű, diszkrét állapotinformációként értelmezhető adatot generál (például: nyitásérzékelés, mozgásdetektálás [78], riasztási állapot [20]), akkor a LoRaWAN kommunikáció műszakilag alkalmas lehet annak továbbítására [79]. Kifejezetten előnyös lehet olyan objektumok esetén, amelyek nagy kiterjedésűek; vagy kültéri helyszínek esetén, ahol a vezetékes kommunikációs alternatívák jelentős többletköltséggel járnának, műszakilag nehezen kivitelezhetőek. [47] A beltéri környezetet is érdemes megvizsgálni, ahol esztétikai és szerkezeti integrációs kérdések merülnek fel. Ha egy vezetékes rendszert utólag kívánnak telepíteni, akkor az a falszerkezet megbontásával vagy külső kábelcsatornás vezetéssel lehetséges [20], ezt többnyire a megrendelők szeretik elkerülni. Erre az esetre jó megoldást jelentenek a vezetéknélküli kommunikációt használó, telepes működésre optimalizált rendszerek, így a LoRaWAN is, feltéve, hogy nincs szükség folyamatos és nagysebességű adatátvitelre [80].

A beléptetőrendszerek és az elektronikus áruvédelmi rendszerek csoportja egyszerű érzékelőknél komplexebb mechanizmusokat foglalnak magukban [81], ahol többször időkritikus, esetlegesen tranzakcióalapú feladatok jelennek meg vagy a folyamatos kapcsolat elengedhetetlen. Szigorúan véve néhány részfunkció megvalósítható lenne LoRaWAN kommunikációval, de ezek részletes vizsgálatával nem foglalkozik az értekezés, így e két csoport is kizárásra kerül.

Külön érdemes kiemelni a távfelügyeleti rendszereket, ahol a leggyakrabban GSM[8]-alapú megoldásokat (alkalmaznak korszerűbb megoldásokat is, de még mindig domináns [82]) alkalmaznak az ismert hibái és korlátjai ellenére. Hátrányai a szolgáltatótól való

[8] GSM: Global System for Mobile Communications – Globális mobil kommunikációs rendszer.

függőség, hálózati leterheltség előfordulása; a GSM rádiós zavarás elleni védelme korlátozott, és megfelelő eszközökkel direkt módon zavarható. [83] A LoRaWAN technológiának, ha a hálózat megfelelően kialakított és konfigurált, akkor nincs szolgáltatótól való függősége. A kétirányú kommunikáció és az üzenetnyugtázás lehetősége alkalmassá teszi a kommunikációt olyan jelzésalapú alkalmazásokra, ahol nem csupán az esemény küldése, hanem annak esetenkénti visszaigazolása is releváns követelmény.

A tisztán személyvédelem kategóriájába eső megoldások, itt is az elektronikus védelmi eszközökre gondolva, ugyanakkor eltérő követelményrendszert támasztanak, mint a tisztán vagyonvédelmi alkalmazások. Amíg vagyonvédelmi rendszerekben egy késleltetett vagy időszakosan kieső jelzés elsősorban anyagi kockázatot okoz, addig személyvédelmi rendszerekben – például egyéni vészjelzők, mobil pánikgombok [84], elszigetelt munkavállalók felügyelete [85] vagy idősellátási riasztórendszerek esetén [86][87][88] – közvetlen emberi élet forog kockán. [20] Más a helyzet a nyomkövető eszközök vonatkozásában, ahol a személyek helyadatai [89][90] kerülnek továbbításra. Ebben az esetben néhány kimaradt koordináta, ha egyébként folyamatos az adattovábbítás, nem okoz közvetlen és azonnali kockázatot. LoRaWAN-t személyvédelmi célra ezért csak abban az esetben tartom alkalmazhatónak, ha a rendszertervezés figyelembe veszi az időkritikus jelzések prioritását, a redundancia szükségességét és a végpontok tápellátásának folyamatos felügyeletét.

A személyek követésére alkalmazott megoldásokhoz hasonló eszközök használhatók mozgó objektumok, vagyontárgyak nyomkövetésére [80] (például: járművek, szállítmányok, konténerek, nagyértékű berendezések vagy ideiglenesen telepített eszközök). Ilyen rendszerek esetén a végpont tipikusan időszakos pozíciófrissítést továbbít a központi rendszer felé. A technológia inkább felügyeleti és állapotmonitorozási célokra, mintsem nagypontosságú, folyamatos mozgáskövetésre szolgál az esetlegesen kimaradó adatok miatt. [91] Itt eltérő következményekkel kell számolni egy személy követéséhez képest, mert ott az időbeli bizonytalanság következménye súlyosabb lehet, mint egy vagyontárgy lokalizációs késleltetése esetén.

Összességében megállapítható, hogy a LoRaWAN kommunikáció elsősorban szenzoralapú, eseményhez kötött, kisméretű adatot továbbító személy- és vagyonvédelmi alkalmazások esetében tekinthető relevánsnak. A technológiának nem célja kiváltani a

már használatos és jól bevált megoldásokat a védelem teljes spektrumában, hanem egyes funkcionális területeken alkalmazható.

1.5 Összegzés, következtetések

Az első fejezettel a célom az volt, hogy összefoglaljam az IoT-alapú kommunikációs megoldások jellemzőit, azon belül is az LPWAN megoldásokat, de kifejezetten a LoRaWAN-t személy- és vagyonvédelmi alkalmazhatóság aspektusában az IoT fogalmából kiindulva.

A három LPWAN kommunikáció (Sigfox, NB-IoT, LoRaWAN) összehasonlító elemzése alapján kirajzolódott, hogy a LoRaWAN hatótávolság, energiahatékonyság, implementációs rugalmasság tekintetében kiemelkedik; kompromisszumos, de a másik két technológiával összevetve, kiegyensúlyozott alkalmazhatóságot kínál. A személy- és vagyonvédelmi alkalmazási területek behatárolása megmutatta azt, hogy a LoRaWAN nem kínál univerzális megoldást mindenre. Kifejezetten érzékelőalapú, eseményvezérelt, kisméretű adatot továbbító rendszerek esetén tekinthető alternatívának, amíg a nagy sávszélesség-igényű vagy folyamatos kommunikációt igénylő alkalmazások túlmutatnak a jellemzőin.

A fejezet szakirodalmi és technológiai áttekintése egyértelművé tette, hogy a LoRaWAN specifikáció elsősorban kommunikációs keretrendszert definiál és a kutatások is főként ezekre fókuszálnak, miközben az alkalmazási következmények, a tanúsított eszközök heterogenitása és a végberendezések életciklus-menedzsmentje kevésbé vizsgált terület. Ez alapozza meg az értekezés 2-5. fejezeteit és az értekezés hipotéziseit.

Az LPWAN technológiák jellemzőinek elemzésével és a LoRaWAN személy- és vagyonvédelem területén való alkalmazásának lehetőségeinek vizsgálatával több megjelent publikációm [20][70][72][74][84][91] is foglalkozik, melyekre nemzetközi hivatkozások is érkeztek.

2 TANÚSÍTOTT LORAWAN ESZKÖZÖK EMPIRIKUS ELEMZÉSE BIZTONSÁGTECHNIKAI ASPEKTUSBÓL

Az előző fejezetben ismertetett szakirodalmi áttekintés rávilágít arra, hogy a LoRaWAN technológia személy- és vagyonvédelmi alkalmazásával kapcsolatos kutatások jellemzően egyedi megoldásokra, konkrét alkalmazási esetekre vagy hálózati szintű vizsgálatokra összpontosítanak, míg a tanúsított végberendezések összességének szerkezeti és működési jellemzői ritkán kerülnek átfogó elemzés tárgyává.

Jelen fejezet célja, hogy a LoRa Alliance által tanúsított LoRaWAN termékeken keresztül megvizsgálja a technológia személy- és vagyonvédelmi alkalmazhatóságának értelmezését. A fejezet a tanúsított eszközök funkcionális szerepét, valós alkalmazásait, működési osztályait, specifikációs besorolását és frekvenciasáv-használatát elemzi, két eltérő időpontban elvégzett saját felmérés eredményeit alapul véve.

A fejezet a következő kutatási kérdésekkel foglalkozik:

- Milyen dominanciák figyelhetők meg funkcionálisan a tanúsított LoRaWAN eszközök között és mi ezeknek a jelentősége személy- és vagyonvédelemben történő alkalmazhatóság vonatkozásában? (Q2.1.)
- Milyen szabványkövetési heterogenitás jellemzi a végberendezéseket és ennek milyen hatása van? (Q2.2.)
- A működési osztályok alakulása mennyiben korlátozza a valós idejű személy- és vagyonvédelmi alkalmazásokat? (Q2.3.)
- Kimutatható-e a folytonos életciklus-menedzsment megléte? (Q2.4.)
- A tanúsítás tényének megléte önmagában elegendő-e a biztonságtechnikai alkalmasság megítéléséhez? (Q2.5.)

Az empirikus elemzés célja nem az egyes eszközök minősítése, hanem olyan visszatérő szerkezeti mintázatok azonosítása, amelyek meghatározzák a LoRaWAN-alapú személy- és vagyonvédelmi rendszerek alkalmazási lehetőségeit és korlátait. A fejezetben feltárt eredmények megalapozzák az értekezés első fő hipotézisének igazolását, és előkészítik a következő fejezetben bemutatott fogalmi keret és biztonságtechnikai kockázati értelmezés kidolgozását.

2.1 A vizsgált eszközkorpusz és az elemzés módszertani kerete

Mint az korábban ismertetésre került a LoRaWAN szabványok kidolgozásáért és a tanúsított eszközökért a LoRa Alliance felel [51]. A Szervezet által közzétett és tanúsított eszközöket vizsgáltam és értékeltem két különböző időpontban elvégzett felmérés eredményei szerint. Az adatforrás alapját a LoRa Alliance által közzétett tanúsított eszközök [92][93] adatlapjai és tanúsítási dokumentumai, hiányos vagy ellentmondó információk esetén pedig a gyártói leírások képezték.

Az első vizsgálat 2020. április 20-án fejeződött be, amikor 177 darab LoRaWAN tanúsított eszközt vizsgáltam meg. [92][94][91] A vizsgálat célja az volt, hogy a termékek alapfunkcionalitását elemezzem és egy, jól elkülöníthető csoportokra épülő taxonómiát alakítsak ki. Ezenkívül vizsgálati szempont volt még, hogy egy adott eszköz milyen LoRaWAN-specifikáció szerint kapta meg a tanúsítást, illetve az eszközök tipikus alkalmazási területei.

A második vizsgálat során a termékek áttekintése 2024. július 27-én fejeződött be, ahol 404 darab eszköz elemzése történt. [92][91] Ennél a kutatásnál az egyik szempont az volt, hogy az aktuális tanúsított eszközök alapján szükséges-e a funkcionális csoportosítást kiegészíteni vagy módosítani. Elemzésre került továbbá, hogy az egyes csoportokban, alkalmazási területeken hogyan változott az eszközök aránya. Egyéb elemzendő aspektus volt, hogy az adott eszköz melyik specifikációra rendelkezik tanúsítással és ezek milyen dátummal születtek, milyen működési osztályba és frekvenciatartományba sorolhatók, alkalmazásra kerül-e további, kiegészítő kommunikáció.

Az elemzéshez közvetlenül és közvetve felhasznált alap eszközjellemzők, -paraméterek:

- megnevezése,
- gyártója,
- mért adat,
- alkalmazási terület,
- kiegészítő kommunikáció,
- specifikáció,
- működési osztály,
- működési frekvenciatartomány,
- tanúsítási jegyzőkönyv dátuma.

Mindkét időszakban végzett elemzés során az elérhető összes releváns adat felhasználásra került. Azt is vizsgáltam, hogy egy adott eszköz esetében történt-e változás, rendelkezésre áll-e egy újabb specifikációs tanúsítás. Előfordultak olyan esetek, hogy helytelen vagy hiányos információk álltak rendelkezésre, amelyeket lehetőség szerint javítottam a gyártói adatok alapján, különben elvetettem.

Az empirikus, strukturális elemzés és összehasonlítás során a trendek, szerkezeti mintázatok és a kockázatok azonosítása volt a cél. A kialakított empirikus adatbázis lehetővé tette, hogy az eszközök tulajdonságai ne önállóan, hanem kockázati interpretációs keretben is értelmezhetővé váljanak, feltárva azokat a kritikus pontokat, melyek a személy- és vagyonvédelem területén való alkalmazás tekintetében relevánsak.

2.2 Funkcionális jellemzők empirikus megoszlása

Ahhoz, hogy az eszközökön elvégezhetők legyenek az összehasonlító és értékelő elemzések, szükségesnek láttam beiktatni egy alapfunkció szerinti kategorizálást, amely még nem a konkrét alkalmazási területre vonatkozik, hanem az eszközök alapfunkciói alapján történik, függetlenül azok aktuális alkalmazási környezetétől vagy felhasználási céljától.

2.2.1 Alapfunkciók szerinti besorolás

A tanúsított LoRaWAN eszközök alapján nyolc ilyen kategóriát határoztam meg. Ezek a következők: LoRaWAN modul, fejlesztői kártya, szenzorcsomópont, beavatkozó csomópont, szenzorinterfész egység, mérőinterfész egység, nyomkövető eszköz, LoRaWAN teszter. A kilencedik kategória a LoRaWAN átjáró lenne, de a vizsgálat időpontjában az átjárókra nem vonatkozott LoRaWAN tanúsítási eljárás. [92]

1. ***LoRaWAN modul***: egy nyomtatott áramköri szerelvény (PCBA - Printed Circuit Board Assembly), amely a LoRaWAN specifikáció követelményeinek megfelelő alapáramköri készletet tartalmaz, és lehetővé teszi a nagy hatótávolságú, alacsony energiaigényű, kétirányú vezeték nélküli kommunikációt. A LoRaWAN modul nem önálló végtermék, hanem a LoRaWAN-alapú alkalmazások fejlesztésének és a késztermékek gyártásának központi hardverkomponense. (AK1)
2. ***Fejlesztői kártya***: olyan nyomtatott áramköri lap (PCB - Printed Circuit Board), amely egy LoRaWAN modult és a működéséhez szükséges kiegészítő áramköröket integrál, és amelyet elsősorban oktatási és prototípus-készítési célokra alkalmaznak. A LoRaWAN fejlesztői kártya önálló mikrovezérlőt is

tartalmazhat, vagy mikrovezérlő-fejlesztői kártyához kapcsolható standard csatlakozóvezetéken keresztül. (AK2)

3. ***Szenzorcsomópont***: olyan késztermék, amely alapvetően három fő egységből áll: érzékelő egységből, feldolgozó egységből és LoRaWAN modulból. A szenzorcsomópont feladata a környezetében bekövetkező specifikus változások érzékelése, azokra történő reagálás és a feldolgozott adatok LoRaWAN hálózaton történő továbbítása. (AK3)
4. ***Beavatkozó csomópont***: olyan késztermék, amely szintén három központi egységből áll: egy beavatkozó egységből, egy feldolgozó egységből és egy LoRaWAN modulból. A beavatkozó csomópont a LoRaWAN hálózaton érkező üzenetek alapján képes meghatározott változást előidézni a környezetében. (AK4)
5. ***Szenzorinterfész egység***: olyan késztermék, amely három fő egységből áll: egy szabványos szenzorcsatlakozóból, egy feldolgozó egységből és egy LoRaWAN modulból. A szenzorinterfész egység szenzor eszközökhöz csatlakoztatható, azoktól adatokat gyűjt, majd az adatokat feldolgozást követően LoRaWAN hálózaton keresztül képes továbbítani. (AK5)
6. ***Mérőinterfész egység***: olyan késztermék, amely egy szabványos mérőcsatlakozót vagy szabványos kommunikációs interfészt, egy adatfeldolgozó egységet és egy LoRaWAN modult integrál. A mérőinterfész egység fogyasztásmérőkhöz csatlakoztatható, azoktól adatokat gyűjt, majd a feldolgozott adatokat LoRaWAN hálózaton továbbítja. (AK6)
7. ***Nyomkövető eszköz***: olyan késztermék, amely három fő egységből áll: egy helymeghatározó egységből, egy feldolgozó egységből és egy LoRaWAN modulból. A nyomkövető eszköz személyek, állatok vagy tárgyak nyomon követésére alkalmas, a helymeghatározási adatokat pedig LoRaWAN hálózaton keresztül továbbítja. (AK7)
8. ***LoRaWAN teszter***: összetett eszköz, amely a LoRaWAN hálózat paramétereinek monitorozására és diagnosztizálására szolgál, különös tekintettel a végberendezésekre és az átjárókra. Kiegészítő funkcióként rádiófrekvenciás (RF - Radio Frequency) teljesítménymérésre is alkalmas lehet. (AK8)

Az ismertetett nyolc darab kategóriát (AK1-AK8) nem tartalmazza egyik LoRaWAN specifikáció vagy hivatalos ajánlás sem, a megvizsgált termékek [92] alapján kerültek kialakításra.

2.2.2 Eszközök alapfunkció szerinti megoszlása

A 2020-ban kialakított nyolc kategória megváltoztatására a 2024-ben elvégzett vizsgálat alapján nem volt szükség [91]. Megállapítható viszont, hogy egyes kategóriák között átfedések fordulnak elő, erre tipikus példa az interfész egységek. Megjelent több olyan termék is, amely nem kizárólag szenzorinterfész egység vagy mérőinterfész egység funkcionalitást tölt be, hanem mindkét szerepnek egyidejűleg megfelel. Ez lehetővé tenné a mérő- és szenzorinterfész egységek összevonását és egy kategóriában történő értelmezését, de az eltérő fő alkalmazási irányok indokolják a külön történő kezelést.

A 2020-ban vizsgált 177 termék közül 2024. július 27-én már csak 129 volt elérhető. [91] Előfordulnak olyan termékek, melyeket már nem forgalmaznak vagy valamilyen okból kivontak a forgalomból, ezért a 2024-es, összesített állapot került figyelembe vételre a további vizsgálatok és következtetések során. Az eszközök besorolásánál a domináns funkcionalitás kapott szerepet.

A 4. táblázat tartalmazza az eszközök alapfunkció szerinti megoszlását a 2020. április 20-ai és 2024. július 27-ei állapotok szerint. A táblázat első részében látható, hogy 2020-ban a szenzorcsomópont (AK3) kategóriába sorolható eszközből volt a legtöbb, 83 darab, de a LoRaWAN modulok (AK1) és a mérőinterfész egységek száma is kiemelkedő. Az is megfigyelhető, hogy bizonyos termékek eltűntek a listából, ahogy azt már korábban ismertettem.

Kategória	**AK1**	**AK2**	**AK3**	**AK4**	**AK5**	**AK6**	**AK7**	**AK8**
2020. április 20.								
Eszközök száma	33	15	83	3	6	24	11	2
2024. július 27.								
Korábbi eszközök száma	19	15	60	2	2	14	7	1
Összesen	49	17	237	9	20	52	15	5

4. táblázat - Alapfunkció szerinti megoszlás a 2020-ban és 2024-ben (Készítette a szerző: [94][91])

A 2020-as állapothoz képest minden kategóriában jelentős növekedés figyelhető meg, vannak kategóriák, ahol közel dupla vagy tripla az eszközök száma. Az arányokban történt legkisebb változás a LoRaWAN modulok (AK1), fejlesztői kártyák (AK2) és nyomkövető eszközök (AK7) tekintetében volt. A modulok és fejlesztői kártyák ugrásszerű növekedésének elmaradása vélhetően arra az okra vezethető vissza, hogy a meghatározó gyártók termékei a LoRaWAN megjelenésének korai szakaszában

elérhetővé váltak és megfeleltek a tanúsítási folyamatnak. Az ezt követő időszakban elsősorban újabb verziók, illetve néhány kisebb gyártó eszközei kerültek piacra. A kizárólag beavatkozó eszközök (AK4) száma továbbra is marginális. A LoRaWAN technológia kétirányú kommunikációra alkalmas, azonban az alkalmazási szinten a legtöbb esetben kizárólag az uplink irány kerül ténylegesen használatra; a downlink kommunikáció jellemzően csak vezérlési és visszajelzési célokat szolgál és ritkábban tényleges beavatkozási célt.

Az 5. táblázat az egyes kategóriák évek szerinti megoszlását foglalja össze. Az év meghatározásakor a tanúsítási jegyzőkönyv dátuma lett figyelembe véve, ahol több jegyzőkönyv is elérhető volt, ott a legkorábbi dátum. 12 olyan eszköz is szerepelt a listában, melyeknek LoRaWAN tanúsítási bizonyítványai nem voltak elérhetők, ezeket az elemzés figyelmen kívül hagyja, hiszen így nem társítható hozzájuk a helyes dátum.

Év	AK1	AK2	AK3	AK4	AK5	AK6	AK7	AK8	Összesen
2016	2	5	2	1	0	0	1	0	**11**
2017	7	3	10	0	2	1	1	0	**24**
2018	7	7	18	1	5	5	3	0	**46**
2019	3	0	22	1	11	1	1	2	**41**
2020	5	2	32	0	11	3	1	0	**54**
2021	5	0	35	2	10	5	4	0	**61**
2022	3	0	59	3	3	4	4	1	**77**
2023	5	0	25	0	5	1	0	1	**37**
2024	11	0	23	1	5	0	0	1	**41**

5. táblázat - Alapfunkciók szerinti megoszlás az évek során (Készítette a szerző: [91])

Látható, hogy az új tanúsított eszközök száma 2016-2018 között folyamatosan emelkedett, de 2019-ben stagnálás (csökkenés) figyelhető meg. 2020-2022 közötti időszakban ismét jelentős növekedés következett be, majd 2023-ra vonatkoztatva ismét lefelé ívelő tendenciát mutatnak az adatok.

A szenzoregységek (AK3) esetében a legmeghatározóbb évek 2020, 2021 és 2022 voltak. 2024-ben több új LoRaWAN modulgyártó is belépett a piacra, ami tükröződik a számokban.

Az alapfunkciók szerinti besorolás és a 2020-as, illetve 2024-es állapotok összehasonlító elemzése alapján megállapítható, hogy a tanúsított LoRaWAN eszközök funkcionális struktúrája a vizsgált időszakban alapvetően stabil maradt, azaz kategóriák illeszkednek a trendekhez. Az eszközpaletta bővülése és módosulása elsősorban a meglévő kategóriákon belül jelentkezett, amely az egyes eszközcsoportokon belüli darabszám

növekedésében, valamint a funkcionális átfedéseket mutató termékek megjelenésében figyelhető meg. A vizsgálat eredményei azt mutatják, hogy a tanúsított eszközkínálat fejlődése nem új funkcionális osztályok kialakulásával, hanem a szenzor- és interfész jellegű megoldások jelenlétének erősödésével, illetve a meglévő kategóriákon belüli komplexitás növekedésével valósul meg, miközben a kizárólag beavatkozási funkciót ellátó eszközök továbbra is elhanyagolható jelenlétet töltenek be.

A következő alfejezet a szürkével jelölt kategóriákra fókuszál (AK3-AK7), azaz nem vizsgálja a LoRaWAN modulokat (AK1), fejlesztői paneleket (AK2) és LoRaWAN teszteket (AK8), mert azok önmagukban vagy funkcionalitásukból adódóan nem részei közvetlenül egy LoRaWAN hálózatnak. Az alapfunkciók szerinti vizsgálat eredményei azt mutatják, hogy a tanúsított LoRaWAN eszközök többsége nem általános IoT eszköz, hanem egy adott feladatra optimalizált, ami a további vizsgálatokat megalapozza.

2.3 Alkalmazás jellege, alkalmazási területek

Mielőtt a LoRaWAN eszközök specifikáció szerinti elemzése történik, fontos megvizsgálni azt, hogy a tanúsított eszközök körében elérhetőek-e olyan termékek, melyek a személy- és vagyonvédelem területén alkalmazhatók. A jelenlegi fejezet az AK3-AK7 alapkategóriákba (333 darab) sorolható eszközökkel foglalkozik [93][94][91], hiszen egy LoRaWAN modul vagy fejlesztői kártya önmagában ilyen szerepet nem tölthet be, csak fejlesztések részét képezhetik és beépülhetnek késztermékekbe (későbbiekben ezért a specifikáció alapú vizsgálatoknál figyelembevételre kerülnek).

Az alkalmazhatóságot jelentősen befolyásolja az eszközök üzemeltetési környezete és az alkalmazás jellege. Eszerint az eszközök csoportosíthatók a felhasználás helye szerint és a telepítés jellege alapján. A vizsgált eszközöket a felhasználás helye szerint három csoportba soroltam be: beltéri, kültéri, vegyes felhasználású. A beltéri és kültéri alkalmazási környezetek értelmezése egyértelmű. Vegyes felhasználású eszközöknek tekintem azokat, amelyek a leírásuk alapján alkalmasak mindkét környezetben működésre. A telepítés jellege szerint két csoportot határoztam meg: fix telepítésűek és mobil eszközök.

A 6. táblázat foglalja össze, a 333 darab eszközt [91][94] a jellemző alkalmazási terület alapján csoportosítva a felhasználás helye szerint és a működési környezet tekintetében. A táblázatban látható, hogy az alkalmazási területek széles spektrumot fednek le.

Telepítés módja	Jellemző eszköztípusok	Személy- és vagyonvédelmi érintettség	Személy- és vagyonvédelmi relevancia
Fix telepítésű beltéri eszközök	• hőmérséklet-, páratartalom-, CO_2-, levegőminőség-szenzorok • jelenlét- és mozgásérzékelők • nyitásérzékelők • vízszivárgás-, füst-, gázérzékelők • villamos-, víz-, gáz- és hőfogyasztásmérők • radiátortermosztátok, okos konnektorok • vészvilágítás állapotjelzők	• behatolásdetektálás (mozgás, nyitás) • tűz- és gázveszély korai felismerése • vízkár megelőzése • jelenlét alapú riasztás és eseménydetektálás	Magas
Fix telepítésű kültéri eszközök	• környezeti- és időjárás-szenzorok • parkolószenzorok • hulladékszintmérők • szivárgásérzékelők • tűzcsap-, sín-, infrastruktúra-monitorozó szenzorok • ipari kontaktus- és állapotfigyelők	• infrastruktúra-védelem • vandalizmus és üzemzavar detektálása • közterületi biztonság támogatása (parkolás, világítás)	Közepes-magas
Fix telepítésű beltéri/kültéri eszközök	• víz-, gáz- és hőfogyasztásmérők • mérő- és szenzorinterfész egységek • analóg/digitális átalakítók	• rendellenes fogyasztási minták (szabotázs, szivárgás) • eszköz- és hálózatállapot megfigyelés • rejtett hibák jelzése	Alacsony-közvetett
Mobil beltéri/kültéri eszközök	• nyomkövetők • személyi badge-ek pánikgombbal • esésdetektálók • gyorsulás- és mozgásérzékelős eszközök • nyomkövető-szenzor kombinációk	• személyvédelem (pánik, esés, eltűnés) • értéktárgy- és járművédelem • jogosulatlan eltávolítás detektálása	Magas-kiemelt

6. táblázat - Tanúsított eszközök alkalmazásspecifikus összefoglalása

Az eszközök legnagyobb része fix telepítésű, ezek elsősorban eseménydetektálási, állapotfelügyeleti feladatot látnak el, mely lehetővé teszi a rendellenességek korai felismerését. Személy- és vagyonvédelem tekintetében ebben a kategóriában jelennek

meg a mozgásérzékelők, a nyitásérzékelők, tűzjellemző érzékelők, jelenlétfelügyeleti eszközök, azaz ebbe a kategóriába tartozó alkalmazások személy- és vagyonvédelmi relevanciája magasnak tekinthető. Bár a kültéri, fix telepítésű eszközök száma alacsonyabb, de relevanciájuk nem elhanyagolható. Ide tartoznak azok a végpontok, amelyek feladata az infrastruktúra-monitorozás, külső területek felügyelete, üzemzavarok és vandalizmus időben történő detektálása. A beltéri és kültéri felhasználásra egyaránt szánt eszközök főleg fogyasztásmérési alkalmazásokhoz kapcsolódnak. Elsődleges feladatuk nem közvetlenül személy- és vagyonvédelmi érintettségű, de közvetve felhasználhatók rendellenes mintázatok detektálására, rejtett hibák felismerésére és jogosulatlan hozzáférés indikálására. A mobil eszközök száma a legalacsonyabb, azonban jelentőségük kiemelkedő. A nyomkövető egységek nem fix helyhez kötött objektumokhoz vagy infrastruktúrákhoz fűződnek, hanem személyekhez, járművekhez vagy mozgó értékhez kapcsolódnak. A pánikgombbal ellátott kitűzők, elesésérzékelők, mozgásmonitorozással kombinált eszközök egyértelműen személyvédelemmel kapcsolatos feladatokat látnak el. Tehát a mobil eszközök személy- és vagyonvédelmi relevanciáját kifejezetten magasnak értékelem.

A vizsgálati eredmények azt mutatják, hogy a LoRaWAN tanúsított eszközök között számos olyan megtalálható, amely közvetlenül vagy közvetve személy- és vagyonvédelmi alkalmazásra készült. A fix telepítésű eszközök a klasszikus elektronikai jelzőrendszer alapját képezhetik, a mobil eszközök tipikusan a személyvédelem területén nyitnak alkalmazási opciókat.

2.4 Specifikáció szerinti értékelés, mintázatok

Ahogy azt korábban ismertettem, a LoRaWAN specifikációk kidolgozásáért, fejlesztéséért és tanúsításáért a LoRa Alliance felel. [51] Az újabb specifikációk megjelenésére elsősorban fejlesztési célból, hibák javítása, valamint pontosítások és értelmezési egyértelműsítések érdekében került sor. A specifikációk határozzák meg mindazon követelményeket, amelyeknek a LoRaWAN eszközöknek és a hálózat elemeinek meg kell felelniük.

2.4.1 Specifikáció mintázatai

A vizsgálat időpontjában hat darab LoRaWAN specifikáció volt elérhető: 1.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, 1.1. Az 1.0 és 1.0.1 specifikációk elavult változatoknak tekinthetők, a jelenleg is aktív verziók az 1.0.2 és az 1.0.4. A LoRaWAN első hivatalos specifikációja,

az 1.0 2015-ben jelent meg [48], majd nemsokkal követte az újabb verzió, az 1.0.1 2016 elején [53]. Tartalmi tekintetben a két dokumentum között nem sok módosítás történt, főleg elírásokat javítottak és pontosításokkal, egyértelműbb magyarázatokkal egészítették ki [53]. Az 1.0.2 változat, mely 2016 közepén jelent meg már hibajavításokat és módosításokat is tartalmaz. [54] Ezt követően 2017-ben került kiadásra az 1.1 specifikáció, amely jelentősebb változásokat eredményezett a korábbi verziókhoz képest. Az apró korrekciókon túl számos funkcionális módosítást is tartalmaz, amelyek többek között az alábbi területeket érintik: keretszámlálók kezelése, eszközosztályok, aktiválási módok, kulcskezelés, valamint a szerverarchitektúra felépítése. [57] A 2018-ban megjelent 1.0.3 verzió átvette az 1.1 specifikáció azon elemeit [55], amelyek a Class B eszközök működéséhez kapcsolódtak. A Class B (beacon-alapú) működés a korábbi verziókban elsősorban elméleti szinten volt jelen [54][95], míg e kiadással gyakorlati síkon is értelmezhetővé vált. A LoRaWAN 1.0.4 specifikáció 2020 októberében jelent meg, és a korábbi 1.0.x verziókhoz képest elsősorban biztonsági és működésbeli pontosításokat, valamint rendszerek közötti együttműködést javító módosításokat vezetett be. Az újdonságok közé tartozik többek között a keretszámlálók és a kulcskezelés szigorítása, a join folyamat egyértelműsítése, valamint a korábban megjelent funkciók egységesebb és gyakorlatban is alkalmazható értelmezése. [56]

A tanúsított LoRaWAN eszközök specifikációk szerinti vizsgálata nem pusztán technológiai összehasonlítást szolgál, hanem lehetőséget ad annak értelmezésére is, hogy az eszközök mennyiben követik azok fejlődését, és ez milyen következményekkel jár a működésük, megbízhatóságuk és védelmi alkalmazhatóságuk szempontjából. A specifikációk egymást követő verziói ugyanis nem kizárólag pontosításokat tartalmaznak, hanem egyes esetekben olyan funkcionális és architekturális változtatásokat is bevezetnek, amelyek közvetlen hatással vannak az eszközök hálózati viselkedésére és jelen értekezés szempontjából releváns jellemzőire.

A 7. táblázat foglalja össze az eszközök specifikáció szerinti megoszlását a 2024-es állapot szerint. [91] A jelenleg már elavultnak számító specifikációk szerint tanúsított eszközök száma minimálisan változott csak, de még mindig elérhetőek, forgalomban vannak. Az 1.0.2 specifikáció szerint tanúsított eszközök jelenléte több, mint háromszorosára nőtt. Az első vizsgálat időpontjában az 1.0.4-es specifikáció még nem létezett, viszont az idő folyamán 6 eszközt újra tanúsítottak a legújabb verzió szerint, négy darabot 1.0.2-ről 1.0.4-re, kettőt pedig 1.0.1-ről 1.0.4-re. [91] Három eszköz 1.0.2 és 1.0.4

szerinti tanúsítással is rendelkezik, ezek a táblázatban az 1.0.4-es oszlophoz lettek besorolva. A legnagyobb darabszámban a 1.0.2 specifikációnak megfelelő eszközök vannak jelen (256 darab), de az 1.0.4-es kategória is jelentős arányaiban. Megjegyzendő, hogy a vizsgált eszközkorpuszban nem jelentek meg 1.1 specifikáció szerint tanúsított végpontok, ami összhangban van azzal, hogy az 1.1 verzió elsősorban hálózati és kulcskezelési szempontból jelent előrelépést, és a gyakorlatban az 1.0.x vonal került implementálásra.

Specifikáció	**1.0**	**1.0.1**	**1.0.2**	**1.0.3**	**1.1**	**1.0.4**
Korábbi eszközök száma	6	31	87	0	0	5
Összes eszköz száma	7	42	256	0	0	96

7. táblázat - Eszközök LoRaWAN specifikáció szerinti csoportosítása (Készítette a szerző: [91])

A 8. táblázat foglalja össze az eszközöket év szerinti bontásban a specifikációk szerint. [91] A táblázat nem tartalmazza azokat az eszközöket, melyekhez a tanúsítási jegyzőkönyv nem volt elérhető a felmérés időpontjában. Jól látható, hogy a tanúsított eszközök specifikációs megoszlása időben eltolódott az újabb LoRaWAN verziók irányába, miközben a korábbi specifikációk fokozatosan kiszorultak az aktív eszközkínálatból. A 1.0.2 szerint tanúsított eszközök száma folyamatosan növekszik. 2020-tól kezdődően viszont egyre több eszköz kapta meg a minősítést 1.0.4 szerint.

	Specifikáció			
Év	**1.0**	**1.0.1**	**1.0.2**	**1.0.4**
2016	4	6	0	0
2017	3	16	4	0
2018	0	6	38	0
2019	0	2	39	0
2020	0	1	50	2
2021	0	11	38	14
2022	0	0	62	18
2023	0	0	11	26
2024	0	0	7	34

8. táblázat - A tanúsított eszközök specifikációja évek szerint (Készítette a szerző: [91])

Megállapítható, ahogy az korábban említésre került, hogy csupán 6 darab termék tanúsítását újították meg, ez azt eredményezi, hogy az utolsó felmérés időpontjában még elérhetők voltak olyan eszközök, melyek elavult specifikáció szerint működnek. Az újratanúsított eszközök alacsony száma arra utal, hogy a gyártók jelentős része nem él az

utólagos tanúsítás lehetőségével, hanem új termékgenerációk bevezetésével követi a specifikációk fejlődését vagy fejlesztés nélkül továbbra is elérhetővé teszik termékeiket.

Összességében megállapítható, hogy a tanúsított LoRaWAN eszközök specifikációs megoszlása időben egyértelmű eltolódást mutat az újabb verziók felé, azonban a korábbi specifikációk szerint tanúsított eszközök továbbra is jelen vannak az aktív piacon. Az empirikus eredmények azt mutatják, hogy a specifikációk fejlődése nem jár automatikusan az eszközök újratanúsításával, ami heterogén specifikációs környezetet eredményez. Ez a jelenség a további fejezetekben vizsgált megbízhatósági és védelmi szempontok értelmezésében kiemelt jelentőséggel bír, hiszen az alkalmazott szabvány és az eszközpark összetétele befolyásoló tényezőként jelenik meg.

2.4.2 Kommunikációs működési osztályok

A 2020-as kutatás külön nem vizsgálta az eszközök kommunikációs osztály szerinti működését, mivel szinte kizárólag csak A osztályú (Class) végberendezések jelentek meg a tanúsított eszközök között. [94] Ez a helyzet 2024-re megváltozott, elérhetők olyan végberendezések, melyek A, A és C, vagy mindhárom osztály szerinti operációra képesek. [91]

A 9. táblázat foglalja össze évek szerint, hogy a tanúsított LoRaWAN végberendezések milyen osztály szerinti kommunikációra képesek.

Kommunikációs működési osztály	**A**	**A, C**	**A, B, C**
2016	10	0	0
2017	23	0	0
2018	44	0	0
2019	41	0	0
2020	52	1	0
2021	60	3	0
2022	78	2	0
2023	26	11	0
2024	31	7	3

9. táblázat - Tanúsított eszközök működési osztályának megoszlása évek szerint (Készítette a szerző: [91])

Az adatok alapján C osztályú működés csak 2020 évtől jelent meg. A vizsgált 2016-2024-es időszakban végig azok az eszközök dominálnak, melyek csak A osztályú kommunikációra képesek. A három darab B osztályú operációra is képes eszköz csupán 2024-ben jelent meg.

A 10. táblázat foglalja össze a tanúsított eszközök osztály szerinti megoszlását a 2024-es állapot alapján. [91] Természetesen minden eszköz képes A osztályú működésre [56], ez specifikációs alapkövetelmény. A táblázat adatai alapján megállapítható, hogy az eszközök több, mint 90%-a kizárólag Class A működésre rendelkezik tanúsítással. Ez nem azt jelenti, hogy ezek az eszközök technikailag ne lennének képesek Class C üzemmódra, hanem azt, hogy erre vonatkozó tanúsítással nem rendelkeznek. A Class A és Class C működésre egyaránt tanúsított eszközök aránya megközelítőleg 6%, míg mindhárom működési osztályra (Class A, B és C) kiterjedő tanúsítással mindössze az eszközök körülbelül 1%-a rendelkezik.

Kommunikációs működési osztály	**Class A**	**Class A, C**	**Class A, B, C**
Eszközök száma	377	24	3

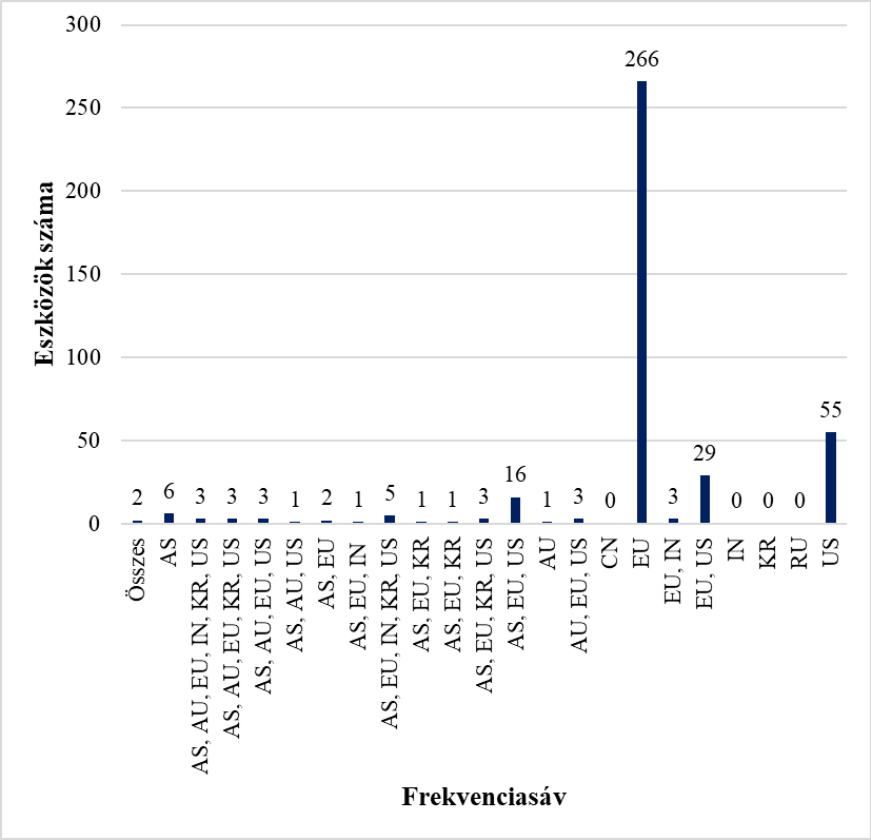
10. táblázat - Tanúsított eszközök működési osztályai (Készítette a szerző: [91])

Összességében megállapítható, hogy a tanúsított LoRaWAN végberendezések kommunikációs osztály szerinti megoszlása a vizsgált időszakban erősen az A osztályú működés irányába tolódik, és ez a dominancia 2024-re sem változott meg érdemben. Bár az utóbbi években megjelentek olyan eszközök, amelyek C osztályú, illetve korlátozott számban B osztályú működésre is képesek, ezek aránya továbbra is alacsony maradt. Az empirikus eredmények arra utalnak, hogy a LoRaWAN-alapú rendszerek túlnyomó többsége továbbra is aszimmetrikus, érzékelésközpontú kommunikációra épül, ahol a downlink-alapú vezérlés és beavatkozás másodlagos szerepet tölt be, azaz nem folyamatos felügyeleti vagy beavatkozási működésre optimalizáltak. Ez a jelenség a későbbiekben vizsgált megbízhatósági, stabilitási és védelmi értelmezések szempontjából szintén meghatározó keretfeltételként jelenik meg.

2.4.3 Frekvenciasávok

A LoRaWAN eszközök vizsgálatánál egy másik fontos szempont lehet az, hogy mely frekvenciasávokra (band) rendelkeznek tanúsítással. Az eszközök tényleges alkalmazási lehetőségei függenek a régiók szabályozási környezetétől [68], illetve azt is megmutatják, hogy mi a gyártói fókusz és a célpiac. Ennek megfelelően, ez az alfejezet a tanúsított eszközök frekvenciasáv szerinti megoszlását vizsgálja.

A 2. ábra foglalja össze, hogy az egyes eszközök mely frekvenciasávokra[9] [91] lettek tanúsítva. 266 olyan eszköz van, amely kizárólag EU band-re kapta meg az engedélyt, de több olyan eset is előfordul, ahol az EU band mellett más is megjelenik (multi-band), ezen eszközök összesített száma 347. Az EU band mellett még az US band kiemelkedő az 55 eszközzel, hozzáadva az US multi-band termékeket is, összesen 127 darab ilyen van. A többi band az EU-hoz és US-hez képest elhanyagolható. [91]



2. ábra - Tanúsított eszközök száma frekvenciasáv szerint (Készítette a szerző: [91])

A frekvenciasáv alkalmazásához kapcsolódóan kiemelendő, hogy az ISM sávokra vonatkozó szabályozás az eszközök rádióhasználatát korlátozza, amely az EU régióban jellemzően 1%. [68]

A vizsgálati eredmények azt mutatják, hogy a gyártók elsősorban az európai piac igényeire optimalizálják eszközeiket. Ebből az következik, hogy a tanúsított eszközök több mint 85%-a alkalmas lehet európai szabályozási környezetben, így Magyarországon történő alkalmazásra is.

[9] Az band-ek rövidítésének magyarázata a Rövidítésjegyzékben került részletezésre.

2.5 Empirikusan azonosított fő szerkezeti mintázatok és azok biztonságtechnikai jelentősége

Az előző alfejezetekben ismertetett empirikus vizsgálatok eredményei átfogó képet adnak a LoRaWAN tanúsított eszközök funkcionális, működési és specifikációs tulajdonságairól. Az ismertetett módszerek és szempontok szerint végzett eszközelemzések lehetővé teszik a magasabb absztrakciós szinten is értelmezhető következtetéseket. Jelen alfejezet célja, hogy integrálja az ismétlődő empirikusan megalapozott szerkezeti mintázatokat és trendeket, melyek a teljes termékpalettára jellemzőek. Az eredmények átvezetnek a személy- és vagyonvédelem területén való alkalmazhatósághoz és kijelöli annak korlátait.

A 404 LoRaWAN tanúsított eszköz empirikus vizsgálata alapján 5 fő mintázatot azonosítottam, melyek a következőkben kerülnek részletezésre.

- ***Alapfunkciók szerinti empirikus mintázat:*** A vizsgált eszközök túlnyomó része érzékelési és mérési funkciót lát el, beavatkozó szereppel rendelkező berendezések száma elhanyagolható. A meghatározott 8 alapfunkció szerinti kategória 2020 és 2024 közötti vizsgálati időszakban strukturálisan nem alakult át, csak arányaiban változott. Megállapítható, hogy a termékkínálatot főként passzív, esemény- és állapotjellegű eszközök alkotják. Ez a LoRaWAN-t a személy és vagyonvédelem területén történő alkalmazási lehetőségekben detektáló technológiaként pozícionálja, nem pedig reagálóként.
- ***Specifikációk követésének empirikus képe:*** A megvizsgált eszközök jelentős része nem a legújabb LoRaWAN specifikáció szerinti tanúsítással rendelkezik. Elenyésző esetben jelennek meg azok a végpontok, melyek rendelkeznek újratanúsítással az aktuális specifikációk szerint. Továbbra is az 1.0.2-es verzió a domináns az 1.0.4-es megjelenésének ellenére és még jelen vannak az elavult 1.0 és 1.0.1-es eszközök is. Az eszközök specifikációs megoszlása időben eltolt és csak részben követi automatikusan a szabványfejlődést. Megállapítható, hogy a specifikációkövetés nem egységes, ami egyazon biztonságtechnikai rendszerben eltérő feltételek szerint működő végpontok egyidejű jelenlétét eredményezheti, és ez a rendszer működésének, kockázatának és megbízhatóságának értelmezésének heterogén állapotát eredményezi.
- ***Működési osztályok dominanciájának mintázata:*** Az A osztályra tanúsított eszközök száma dominálja a piacot, a vizsgált minta alapján ez 90% feletti. A C

és B osztályú működés időben jelentősen eltolva jelenik csak meg és számuk elenyésző, kifejezetten igaz ez a B osztályú működésre. A LoRaWAN tanúsított végberendezések működése nem folyamatos elérhetőségre optimalizált, amely személy- és vagyonvédelmi szempontból korlátozza az azonnali, valós idejű beavatkozás lehetőségét és a folyamatos elérhetőség is strukturális korlátokba ütközik.

- ***Régiós-frekvenciasáv fókusz mintázata:*** A vizsgált eszközök jelentős része EU frekvenciasávra tanúsított és a multi-band termékek túlnyomó többsége szintén EU kompatibilis. A további régiók jelenléte arányaiban nem számottevő, azaz a végberendezések elsődlegesen európai alkalmazásra optimalizáltak. A minta lehetővé teszi a magyarországi alkalmazások széleskörű adoptációját. Azonban itt fontos megjegyezni még az 1%-os korlátozást is, ami tovább erősíti, hogy a technológia eseményvezérelt, nem pedig folyamatos kommunikációra alapozott, ami a személy- és vagyonvédelmi alkalmazások tervezése során ismert kockázati tényezőként jelenik meg.
- ***Életciklus-stabilitás mintázata:*** A 2020-as vizsgálat során jelenlévő eszközök egy jelentős része, közel egyharmada már nem volt elérhető, a 2024-es időpontban, de a funkcionális struktúra megmaradt. Az eszközkínálat dinamikusan változik, ami a működési logikát nem, csak az eszközszámot érinti. Az eszközök mérhető szánú fluktuációja is közvetlenül indokolja az életciklus-alapú megközelítés szükségességét.

Az empirikus vizsgálat alapját csak LoRaWAN tanúsított eszközök képezték, melyet alapvető szintnek tekintek egy személy- és vagyonvédelem területén történő alkalmazás esetén, de egyértelműen kijelenthető, hogy a tanúsítás megléte nem jelent ekvivalenciát a megfelelőséggel, számos rejtett kockázati mintát tárt fel az összehasonlító elemzés.

2.6 Összegzés, következtetések

A 2. fejezet empirikus elemzése és a feltárt mintázatok azt mutatják, hogy a tanúsított LoRaWAN végberendezések kínálata funkcionálisan passzív, specifikációban heterogén, működésében eseményvezérelt, és életciklusában dinamikus. E fejezetben tett megállapításaim alapján igazoltam az értekezésben megfogalmazott első hipotézist (H1), miszerint a tanúsított LoRaWAN végpontok ökoszisztémája olyan strukturális mintázatokat mutat, amelyek alapvetően meghatározzák a személy- és vagyonvédelmi rendszerekben történő alkalmazásának korlátait. Kimutattam a detektálásközpontú

működést, az eseményvezérelt kommunikáció korlátait, a specifikációs és működési heterogenitást és következményeit, valamit az életciklus-változás hosszútávú jelenlétét.

A hipotézis igazolásához felhasznált eredmények [94][91][96] saját publikációimban adtam közre, melyekre több nemzetközi hivatkozás is érkezett.

3 FOGALMI KERET, DEFINÍCIÓK ÉS CSOPORTOSÍTÁSOK

A 2. fejezetben ismertetett empirikus elemzések jól szemléltetik azt, hogy a tanúsított LoRaWAN termékek kínálata azonosítható mintázatokat mutat, és ezek közvetlen hatással vannak a személy- és vagyonvédelem területén történő alkalmazhatóságukra. A feltárt funkcionális jellemzők, eseményvezérelt működés, specifikációs heterogenitás és az életciklus-változás önmagukban és külön-külön nem értelmezhetők egységes biztonságtechnikai szemléletű keretben.

A személy- és vagyonvédelem területén alkalmazott IoT-alapú rendszerek esetében nem elégséges a technológia vagy kommunikációs szintű elemzés; szükségessé válik egy olyan fogalmi és értelmezési keret, amely képes az IoT sajátosságokat megbízhatósági, kockázati és üzemeltetési szempontból is összekötni. A 2. fejezet eredményei alapján indokolt egy ilyen keretrendszer kidolgozása.

Jelen fejezet célja, hogy a korábban ismertetett megállapításokra építve meghatározza ezen alapfogalmakat és kockázati kategóriákat. A fejezetben bevezetett fogalmak általános IoT-alapú elektronikai védelmi rendszerekre vonatkoznak, ugyanakkor azok értelmezése és alkalmazhatósága jelen értekezésben a LoRaWAN-alapú rendszerek empirikus vizsgálatán alapulnak. Ennek megfelelően a kiterjesztése hasonló működési és kommunikációs sajátosságokkal rendelkező IoT rendszerek körére értelmezhető.

Jelen fejezet a következő kutatási kérdésekre épül:

- Lehet-e értelmezni az IoT-alapú védelmi rendszert egységesen, ami több, mint a tisztán kommunikációs infrastruktúra-szemlélet? (Q3.1.)
- Meghatározható-e egy többdimenziós biztonságtechnikai modell a végpontok megbízhatóságára? (Q3.2.)
- Formalizálható-e a megbízhatósági modell a dimenziókra építve és azokat további paraméterekre bontva? (Q3.3.)
- Levezethető-e a megbízhatósági modellből a végpontok funkcionális kockázati besorolása? (Q3.4.)
- A kidolgozott modell alkalmas-e, hogy a végpontokat összehasonlítóan, rendszerszintű szemléletben értékelje? (Q3.5.)

A fejezet a bevezetett fogalmi keret eredményeként, az IoT-végpontok megbízhatóságát nem izolált műszaki paraméterként, hanem rendszerszintű, kockázati kontextusba ágyazott tulajdonságként teszi értelmezhetővé. Ez készíti elő a végpontok validációját és alkalmazási következtetéseket.

3.1 IoT-alapú elektronikai védelmi rendszer

Az ISO/IEC 30141 nemzetközi ajánlás általános architekturális megközelítése [28] jó kiindulási alapot biztosít az általános IoT rendszerek értelmezésére, azonban a személy- és vagyonvédelmi alkalmazások speciális igényei indokolják annak kiterjesztését. Ha figyelembe vesszük a szabványban felvázolt IoT struktúrát és az elektronikai védelmi rendszerek sajátosságait, akkor megalkotható az IoT-alapú elektronikai védelmi rendszer fogalmi környezete.

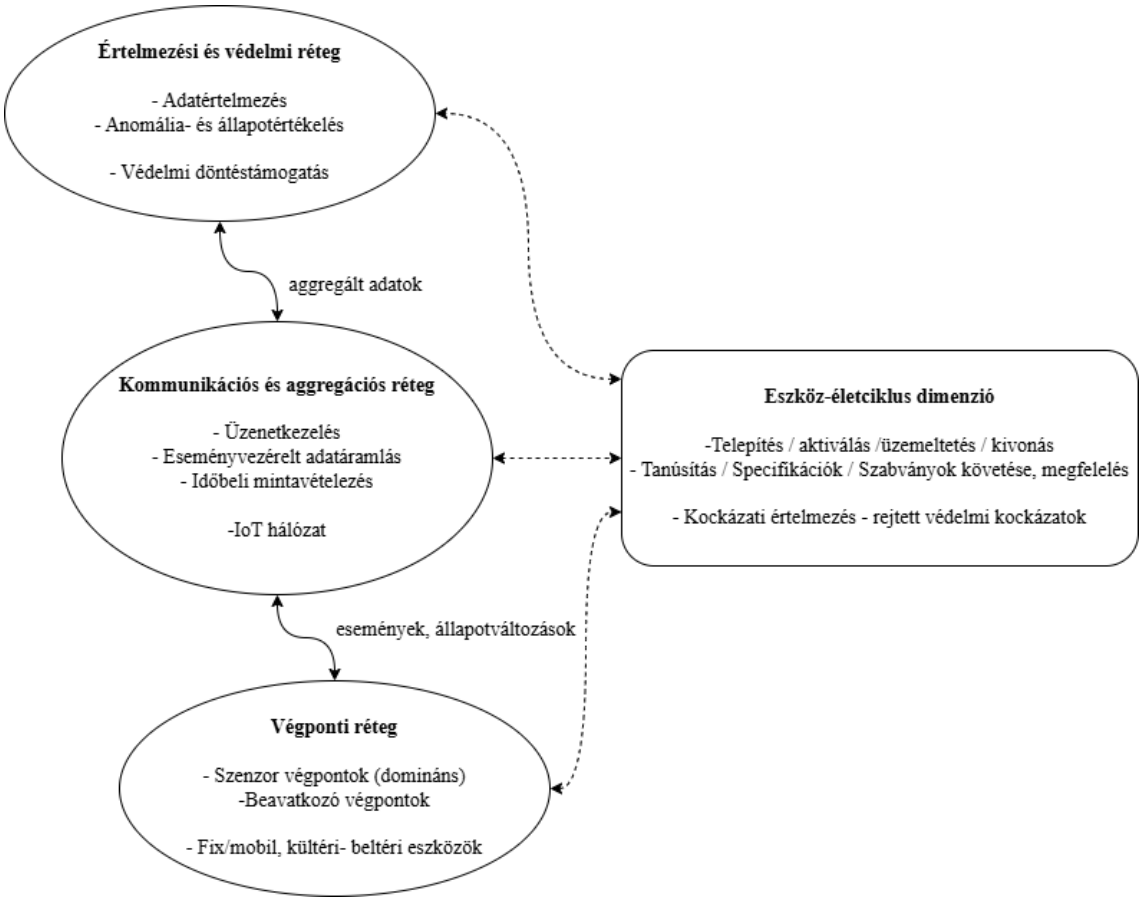
Az ismertetett empirikus vizsgálatok megmutatták, hogy a végberendezések jelentős része funkcionálisan passzív szerepet tölt be. Az eszközök elsődleges funkciója az értékelés és állapotjelzés, ezzel szemben a beavatkozásra dedikált végpontok száma elenyésző. A vizsgált eszközbázis másik meghatározó tulajdonsága az eseményvezérelt működés. A végpontok általában nem folyamatos adatátvitelt valósítanak meg, hanem meghatározott eseményekhez, állapotváltozásokhoz kötötten vagy periodikusan kommunikálnak. Ez személy- és vagyonvédelem szempontjából azt eredményezi, hogy a környezet megfigyelése csak diszkrét mintavételezésen alapul. Ez a kockázatok értékelésében és a megbízhatósági keretrendszer szempontjából jelentős.

A 2. fejezet eredményei továbbá még rámutattak arra is, hogy a végberendezések szabványban, specifikációban, működésben és életciklusban heterogenitást mutatnak. Azaz egy IoT-alapú elektronikai védelmi rendszerben is jelen lehetnek eltérő szabványverzióknak, kommunikációs módnak és életciklus-állapotnak megfelelő eszközök. Ez a heterogenitás nem számít speciális esetnek, ahogy az ISO/IEC 30141 is kimondja [28], ezt figyelembe kell venni az IoT rendszerek esetén. Eszerint a megbízhatóság kérdésköre biztonságtechnikai aspektusból komplex, rendszerszintű megközelítést igényel.

Tehát az IoT-alapú elektronikai védelmi rendszerek nem csupán kommunikációs infrastruktúraként értelmezhetők, hanem olyan komplex rendszerként, ahol a végpontok funkcionális jellege, konkrét alkalmazása, működési módja, szabványnak vagy specifikációnak való megfelelése és életciklusának összessége határozza meg a tényleges

védelmi képességét. Ez az értelmezési megközelítés összhangban van a ISO/IEC 30141 szerinti referenciaarchitektúrával, ami az IoT rendszereket elosztott, rétegekre épülő életciklus-orientált struktúrában kezeli [28], kiemelve az egyes komponensek közötti kölcsönhatások fontosságát.

A 3. ábra az IoT-alapú védelmi rendszer fogalmi modelljét szemlélteti. A védelmi funkció elosztott módon a végponti eszközökre, rétegre épül, de a tényleges értelmezés és döntés magasabb rendszerszinteken valósul meg. Ahogy azt az ábra is szemlélteti a fogalmi keretet három rétegben modelleztem, figyelembe véve az ISO/IEC 30141 IoT architekturális javaslatait, klasszikus hálózati topológiákat és modelleket átültetve a jelenleg vizsgált környezetbe. De, azokat nem közvetlenük vettem át, hanem a jelen értekezés fogalmi és biztonságtechnikai kontextusához illesztve alkalmaztam. Az eszköz-életciklus nem önálló architekturális rétegként jelenik meg, hanem a rendszer egészére kiterjedő, időben változó dimenzióként, amely a komponensek működését és megbízhatósági értelmezését egyaránt befolyásolja. [72]



3. ábra - IoT-alapú védelmi rendszer fogalmi modellje

Összességében megfogalmazva: ***IoT-alapú elektronikai védelmi rendszer*** alatt olyan elosztott, hálózatba kapcsolt érzékelő- és végponti rendszert értek, amelynek elsődleges célja nem az adatgyűjtés, hanem képes védelmi események detektálására, jelzésére és tipikusan vezeték nélküli kommunikációt alkalmazva továbbítására, jellemzően korlátozott kommunikációs és energiaforrások mellett. A rendszer alapvető jellemzője, hogy a védelmi funkció nem egyetlen központi eszközben valósul meg, hanem több, egymással együttműködő végpont és háttérrendszer kölcsönhatásának eredményeként jön létre heterogén környezetben. Ezek a rendszerek tipikusan jelenlét-, mozgás-, behatolás- [96] vagy állapotváltozás-alapú eseményeket figyelnek, és a riasztási információkat központi feldolgozó vagy felügyeleti rendszer felé továbbítják.

Jelen értekezés az IoT-alapú elektronikai védelmi rendszer fogalmát általánosan kezeli, de meg kell jegyezni, hogy annak kidolgozása a 2. fejezet LoRaWAN-alapú empirikus vizsgálatára épül. A fejezetben megfogalmazott rendszer értelmezése alkalmazható minden olyan, IoT-alapú elektronikai védelmi rendszerre, mely hasonló működési sajátosságokkal rendelkezik.

3.2 IoT végpont biztonságtechnikai megbízhatósága

Az előző fejezetben ismertetett fogalmi modell az IoT-alapú védelmi rendszereket három, egymásra épülő réteg mentén írja le, amelyek közül a végponti réteg a rendszer elsődleges adatforrását jelenti. Ennek megfelelően a jelen fejezet a továbbiakban kifejezetten a végpontokra koncentrál, és azok megbízhatóságát értelmezi biztonságtechnikai nézőpontból.

A szakirodalmi feldolgozás (1. fejezet), valamint a 2. fejezetben bemutatott empirikus eredmények alapján megállapítható, hogy a klasszikus műszaki, IT- és ICT-rendszerekben (IT – Information Technology: Információs technológiák) alkalmazott megbízhatósági fogalmak az IoT végpontok esetében önmagukban nem elegendőek változtatás nélkül. [20] Az IoT végpontok sajátos működési jellemzői és alkalmazási környezete indokolttá teszik e fogalmak kiterjesztését és újraértelmezését biztonságtechnikai kontextusban. A fejezet célja egy ilyen megközelítés megfogalmazása, amely alapot biztosít a további alfejezetekben tárgyalt, a megbízhatóságot befolyásoló tényezők rendszerezéséhez, valamint a kockázati osztályozási keret kialakításához.

3.2.1 Szabvány-alapú megközelítés az IoT-végpont megbízhatósági értelmezéséhez

Az IoT végpontok biztonságtechnikai megbízhatósága fogalmi keretének meghatározásához jó kiindulási alapot biztosít a kapcsolódó szabványok figyelembe vétele. Bár ezek a szabványok nem feltétlenül IoT-specifikus technológiákra és megoldásokra születtek, de szemléletükben és fogalomrendszerükben kapcsolódhatnak és releváns párhuzamot biztosíthatnak.

Biztonságtechnikai szabványok közül az egyik legrelevánsabb az értekezés témáját tekintve az MSZ EN 50131 szabványsorozat, amely a behatolásjelzőrendszerek követelményeit foglalja össze. [97] A szabványsorozat a megbízhatóságot nem pusztán működőképességként, hanem kockázati környezethez kapcsolt védelmi alkalmasságként írja le. A szabvány által alkalmazott, különböző szintekhez rendelt követelményrendszer átültethető IoT környezetbe úgy, hogy egy végpont megbízhatóságánál figyelembe vesszük az alkalmazási környezetet és a védelmi funkciót egyaránt.

Bár csak közvetve kapcsolódik, de hasonló szemlélet jelenik meg az MSZ EN IEC 62676 szabványsorozatban is, amely a videómegfigyelőrendszerek követelményeit írja le. A szabvány megkülönbözteti azokat a videómegfigyelő rendszereket, melyek technikailag működőképesek, azoktól a rendszerektől, amelyek biztonságtechnikai célra alkalmasak. A szabvány kiemeli, hogy a szolgáltatott információ önmagában nem elegendő, annak értelmezhetősége, megbízhatósága és kontextushelyessége is meghatározó szempont. [98] A szabvánnyal való kapcsolódási pont, hogy bár egy végpont működése technikailag megfelelő lehet, de biztonságtechnikai szempontból bizonytalanná válhat.

Az ISO/IEC 27005 szabvány az információbiztonsági kockázatkezelés témakörével foglalkozik, viszont szintén releváns szemléletet kínál. A szabvány a megbízhatóságot és a biztonságot kontextusfüggő, kockázaton alapuló megközelítésben értelmezi. [99] A logikája, amely az eszközök, fenyegetések és következmények összeségére épít, felhasználható az IoT végpontok esetében is. Miszerint, a végpont által szolgáltatott adat értéke nem abszolút, hanem a helyzettől és a környezettől egyaránt függ.

Az MSZ CLC IEC/TS 62443 szabványcsalád, amely az ipari automatizálási rendszereknél használatos, az eszközök életciklus-menedzsment szemléletében és a rendszerek heterogén felépítésének kezelésében nyújt kapcsolódást. A szabvány kiemeli, hogy az eszközök megbízhatósága az életciklusuk során folyamatosan változik és a

kivonásuk (kivonás elmaradása) vagy részleges üzemeltetésük rejtett kockázatokhoz vezethet [100]. Ez a szemlélet előrevetíti a későbbi, életciklus-menedzsment fontosságával foglalkozó fejezetet és a kivonási eljárás relevanciáját.

Az ETSI EN 303 645 rámutat azokra a kritikus pontokra, melyek a klasszikus értelmezésekből legtöbbször kimaradnak, ilyen az életciklusvégi állapotok kezelése, az alapértelmezett konfigurációk problémái és a frissíthetőség korlátjai. [27] Ez alapvetően fogyasztói IoT termékekre vonatkozik, de átültethető belőlük, hogy az IoT végberendezések biztonságtechnikai megbízhatósága nem választható el az életciklus-kezeléstől.

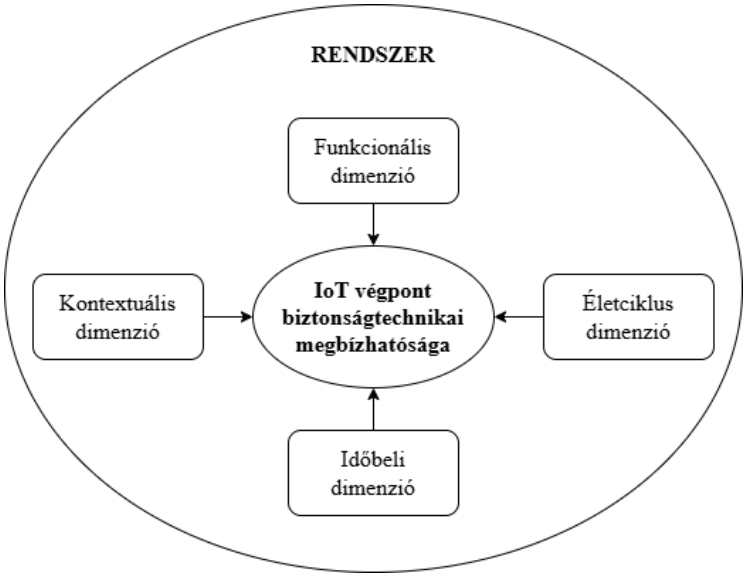
A már korábban megvizsgált és felhasznált ISO/IEC 30141 IoT referenciaarchitektúra a megbízhatóságot nem különíti el az egyes részegységek szerint, hanem az IoT rendszerek általános minőségi jellemzőjének tekinti [28], ami a végpontok, a kommunikációs infrastruktúra, és menedzsmentfunkciók összességéből tevődik össze.

Összességében megállapítható, hogy bár az imént összefoglalt szabványok, leírások és ajánlások eltérő területekről kerültek összegyűjtésre, de mégis mindegyiknek van kapcsolódási pontja egymással és az IoT végpontok biztonságtechnikai megbízhatóságával. Általánosságban, a megbízhatóságot nem tisztán műszaki tulajdonságként vagy kommunikációs jellemzőként értelmezik, hanem kockázati környezethez és funkcióhoz kötötten. Ezeket felhasználva és átültetve az értekezés témájába, meghatározható az IoT végpontok biztonságtechnikai megbízhatósága.

3.2.2 Megbízhatóság értelmezése

Az IoT végpont biztonságtechnikai megbízhatóságának megfogalmazásakor nem lehet pusztán a műszaki megközelítésre építkezni vagy a kommunikációs képességet vizsgálni.[20][85][94] Ezek az eszközök eseményérzékenyek és környezetfüggők. A fogalomnak azt kell kifejeznie, hogy a végpont által szolgáltatott adat alkalmas-e az adott állapot helyes értelmezésére és a döntések megalapozására. Egy IoT végpont technikailag úgy is működőképes lehet, hogy az általa továbbított adatok személy- és vagyonvédelmi szempontból nem egzaktok, hiányosak vagy időben relevanciájukat vesztették. Azt kell figyelembe venni, hogy az adott eszköz helyes állapotot közöl-e, a közölt információ értelmezhető-e a döntésekhez, illetve torzítja-e a védelmi képet. Mivel a személy- és vagyonvédelemben alkalmazott IoT végpontok fő feladata nem a beavatkozások végzése, hanem állapotinformációk továbbítása, ezért az IoT végpontok biztonságtechnikai

megbízhatóságát nem elég egy abszolút tulajdonságnak tekinteni, hanem függ a működési környezettől, az aktuális életciklus állapotától és a rendszerbe ágyazottságtól.



4. ábra - Megbízhatóság dimenziói

Az IoT végpontok biztonságtechnikai megbízhatóságát 4+1 dimenzióra osztottam fel, ahogy azt a 4. ábra is szemlélteti. Az első ilyen dimenzió a ***funkcionális dimenzió***, itt jelenik meg az adott eszköz alapvető funkcionális képessége, miszerint milyen eseményeket képes érzékelni és továbbítani. Ez egy összetett dimenzió, mivel részét képezi az érzékelők minősége és megbízhatósága, a hardver-szoftver egysége, a konfigurációk megfelelő megléte, tanúsításoknak, szabványoknak való megfelelés. [91][20] A második dimenzió az ***időbeli dimenzió*** mely bár függ a kommunikáció stabilitásától és a hálózati környezet megfelelőségétől, de nem csupán technikai paraméterek eredője. Ez a dimenzió nem a kommunikáció meglétét modellezi, hanem annak időbeli hatását. [101] A kapcsolódó hatások és tényezők lehetnek a késleltetés, csomagvesztés, időbeli korlátozások (duty cycle), interferencia és hálózati instabilitás. Egy késve érkezett, bár technikailag sikeresen továbbított adat értéktelenné válhat. A harmadik a ***kontextuális dimenzió***, amely azt szemlélteti, hogy az adott végpontot milyen környezetben alkalmazzuk és ott milyen feladatot lát el. Az ide tartozó és releváns szempontok, hogy a végpont hol van elhelyezve, a környezetének fizikai struktúrája, sajátosságai és a működési közeg. [9] [94][101][102][103] Azaz, ugyanaz a végpont más környezetben eltérő megbízhatósági szintet jelenthet. A negyedik egy időben kiterjesztett dimenzió, az ***életciklus dimenzió***, mely dinamikusan értelmezendő. Kapcsolódó befolyásoló tényezők a telepítés, üzemeltetés, módosítások, frissítések és az eszközök

megfelelő kivonása [72][104]. Tehát a megbízhatóság nem statikus tulajdonság, hanem az életciklus során folyamatosan változó tényező. Ezek a dimenziók hatással vannak egymásra és nem elhanyagolható a rendszerszintű szemlélet, beágyazottság sem, hiszen egy végpont nem izolált elem, hanem egy rendszer része, de jelen értekezés a rendszer többi elemét külön nem, csak szükséges összefüggéseiben vizsgálja és elemzi.

Összességében megfogalmazva: Az ***IoT végpont biztonságtechnikai megbízhatósága*** az adott eszköz azon képességének összessége, amely biztosítja, hogy a végpont a személy- és vagyonvédelmi szempontból releváns eseményeket és állapotváltozásokat a működési környezethez és védelmi funkcióhoz igazodva időben, torzításmentesen és értelmezhető módon továbbítja, úgy, hogy a kommunikációs sajátosságok, az alkalmazási környezet vagy életciklusbeli eltérések nem vezetnek téves, elmaradó vagy félreértelmezett védelmi döntésekhez. [20][105][70][84][102][72][9][104][94]

3.2.3 Megbízhatósági dimenziómodell formalizálása

Általánosságban az IoT végpontok biztonságtechnikai megbízhatósága a következő általános alakkal formalizálható:

$$R_{sec}(e,t) = f(F_e, T_e, C_e, L_e(t), S_e) \tag{1}$$

$$R_{sec}(e,t) = w_F F_e + w_T T_e + w_C C_e + w_L L_e(t) + w_S S_e \tag{2}$$

$$w_F + w_T + w_C + w_L + w_S = 1 \tag{3}$$

ahol,

- e - IoT végpont,
- t - idő, időfüggés,
- R_{sec} - IoT végpontok biztonságtechnikai megbízhatósága,
- F_e - funkcionális dimenzió,
- T_e - időbeli dimenzió,
- C_e - kontextuális dimenzió,
- L_e - életciklus dimenzió,
- S_e - rendszerbe ágyazottság, rendszerszintű kiterjesztés,
- w_i – súlyparaméterek.

A modell célja nem egy abszolút megbízhatósági szám előállítása, hanem egy megbízhatósági index létrehozása személy- és vagyonvédelem területén alkalmazott IoT végpontok értékelésére, amely az egyes dimenziók, elemek normalizált értékének súlyozott átlagából tevődik össze. Az eredmény egy 0 és 1 közé eső szám, mely relatív összehasonlításra alkalmas és leképezhető kockázati osztályba, amivel a következő fejezet foglalkozik.

Funkcionális dimenzió (F)

A funkcionális megbízhatóság annak mértéke, hogy a végpont képes-e a releváns események helyes detektálására, ami magában foglalja a már korábban ismertetett alapvető technikai működési paramétereket, valamint a szabványoknak és specifikációs követelményeknek való megfelelést.

Formálisan értelmezve ezen paraméterek súlyozott összegeként:

$$F_e = \alpha_1 D_e + \alpha_2 I_e + \alpha_3 V_e \tag{4}$$

ahol:

- D_e - detektálási pontosság,
- I_e - jelértelmezési integritás,
- V_e - validált működési megfelelőség, konfiguráció (tanúsítás, szabvány),
- α_i - súlyparaméterek.

Időbeli dimenzió (T)

Az időbeli tényező annak mértékét fejezi ki, hogy az információ megfelelő időablakon belül érkezik-e.

$$T_e = P(\Delta t_e \leq \Delta t_{crit}) \tag{5}$$

ahol:

- P – valószínűség (becsült),
- Δt_e - tényleges késleltetés,
- Δt_{crit} - adott védelmi funkció kritikus időhatára.

Ha egy LoRaWAN kommunikációt alkalmazó személy- és vagyonvédelmi eszközt veszünk figyelembe, akkor ez a paraméter erősen függ például a duty cycle-től,

interferenciától, hálózati elérhetőségtől. Ez a mutató nem csupán a kommunikáció meglétét reprezentálja, hanem annak személy- és vagyonvédelmi időszerűségét.

Kontextuális dimenzió (C)

Ez a dimenzió a végpont működését meghatározó alkalmazási és fizikai környezetet jellemzi. Ide tartozik a végpont elhelyezése (pl. beltéri/kültéri), a környezet fizikai struktúrája és a működési közeg:

$$C_e = \gamma_1 E_e + \gamma_2 A_e \tag{6}$$

ahol:

- E_e - fizikai elhelyezés és környezeti jellemzők (beltér/kültér, strukturális adottságok),
- A_e - alkalmazás jellege és működési környezete,
- γ_i - súlyparaméterek.

Ez a paraméter nem egy adott eszköz abszolút jellemzője, hanem függ az alkalmazási közegtől, környezettől. Tehát ugyanazon végpont más környezetben eltérő kontextuális értéket vehet fel.

Életciklus dimenzió (L)

Az életciklus-megbízhatóság az időben változó kitettséget reprezentálja, amely függ az eszköz frissítésének állapotától, a konfiguráció megfelelőségétől és a gyártói támogatottságtól:

$$L_e(t) = \delta_1 U_e(t) + \delta_2 Cfg_e(t) + \delta_3 Sup_e(t) \tag{7}$$

ahol:

- $U_e(t)$ – beágyazott szoftver/frissítés állapota,
- $Cfg_e(t)$ - konfiguráció megfelelősége,
- $Sup_e(t)$ - gyártói támogatottság,
- δ_i - súlyparaméterek.

Bár a formula többi eleme is mutathat időfüggést, itt van kifejezetten nagy jelentősége, ezért kerül külön jelölésre.

Rendszerbe ágyazottság, rendszerszintű kiterjesztettség (S)

A rendszerbe ágyazottság annak a mutatója, hogy egy végpont kiesése milyen mértékben befolyásolja a védelmi rendszer működőképességét.

Ez három, jól elkülönülő komponensre bontható:

$$S_e = \rho_1 N_e + \rho_2 Dep_e + \rho_3 Q_e \tag{8}$$

ahol:

- N_e - hálózati struktúra,
- Dep_e - függőségi hatás,
- Q_e - aggregációs/döntési hatás,
- ρ_i - súlyparaméterek.

A fejezetben ismertetett megközelítés rávilágít arra, hogy a megbízhatóság nem egy abszolút tulajdonság, nem redukálható egyetlen paraméterre, hanem az adott személy- vagy vagyonvédelmi feladattól és a kockázati környezettől függő. Ennek megfelelően, a következő rész funkcionális végpont-kockázati osztályozási keretet vezet be, amely erre az alfejezetre építve lehetővé teszi az IoT végpontok strukturált, biztonságtechnikai aspektusú besorolását.

3.3 IoT funkcionális végpont-kockázati osztály

Az előző fejezetben megfogalmazott megbízhatósági értelmezés rámutatott arra, hogy az adott IoT végpont technikai jellemzőit, a kommunikációs és hálózati környezetét, alkalmazási és biztonságtechnikai aspektusát, valamint az életciklus menedzsmentjét együttesen kell kezelni. Ennek következtében egyazon IoT végpont eltérő kockázati besorolás alá eshet aszerint, hogy milyen személy- vagy vagyonvédelmi feladatot lát el. [20]

A 2. fejezet által ismertetett empirikus elemzés eredményei [94][91] és a kapcsolódó ajánlások rámutattak arra, hogy a végpontok funkcionálisan (és egyéb szempontok alapján is) heterogének, amely nem alapvető hibának tekinthető, hanem

biztonságtechnikai szempontból kockázati tényezőnek, ha az adott végpont funkciója, megbízhatósága és védelmi szerepe nem az alkalmazási környezetnek megfelelő.

Mindezek alapján szükségesnek látom egy olyan kockázati osztályozási szempontrendszer bevezetését, amely figyelembe veszi azt, hogy az adott végpont milyen védelmi funkciót lát el, a környezetét és milyen következményekkel jár, ha az általa szolgáltatott információ sérült, hiányos vagy késleltetett. Azt meg kell jegyezni, hogy a kockázati osztályok meghatározása nem azonos egy klasszikus kockázatértékeléssel, de felhasználja annak alapmódszereit. Az IoT funkcionális végpont-kockázati osztály az előzőekben ismertetett megbízhatóság következmény-értelmezése.

3.3.1 Funkcionális végpont-tipológia

A kockázati osztályok meghatározásának alapvető kiindulási pontja a jelzett esemény következménye és hatása [74][106][107]. Az eredmény súlyossága nem csak a technológiai paraméterektől függ, hanem összekapcsolható a végpont szerepével.

Kiemelendő, hogy a 2. fejezetben alkalmazott osztályozás (funkcionális alapkategória) [94] az empirikus vizsgálatokon alapuló rendszertechnikai szemléletű volt, amely a fejezet eredmény-struktúrájának kiindulási pontját adta. Ebben az alfejezetben bevezetett tipológia a 2. fejezet eredményeiből kiinduló védelmi funkció-alapú megközelítés, amelyet a kockázati osztály értelmezésekor a következmény, hatás megalapozására használok fel. Tehát, a két kategorizálás értelmezése más absztrakciós szinten történik, nem egymás alternatívái, de egymásból levezethetők.

Az IoT végpontok funkciójuk alapján a következő általános kategóriákba sorolhatók:

- ***Állapotjelző vagy információs végpontok***: olyan érzékelők, melyek környezeti állapotot jeleznek, funkciójuk elsősorban információszolgáltató jellegű. Rendellenes működésük nem okoz közvetlen védelmi sérülést, de befolyásolja a helyzetérzékelést. Ilyen végpont lehet például egy hőmérsékletmérő vagy egy jelenlétérzékelő. Ide tartozhatnak AK3 szenzorcsomópont és AK5 szenzorinterfész alapkategóriák egyes elmei.
- ***Felügyeleti és trendalapú végpontok:*** olyan eszközök, melyek hosszabbtávú állapotmegfigyelést végeznek. Kockázatuk alacsony és nem azonnal, hanem hosszútávon érvényesül, kumulatív jellegű. Ilyen lehet egy fogyasztásmérő vagy egy degradáció felügyelő eszköz. Az alapkategóriák közül tipikusan az AK6

mérőinterfész elemei tartoznak ide, de az AK3 és AK5 egyes eszközei is érintettek lehetnek.

- ***Beavatkozást végző végpontok:*** Fő feladatuk az aktív vezérlés ellátása, hibás működésük fizikai következményekkel is járhat. A funkciójukból adódóan legtöbbször magas következményszinttel bírnak. Ilyen eszközök lehetnek például a relék, amik valaminek a kapcsolását végzik. Ide sorolhatók az AK4 beavatkozó csomópont alapkategória végpontjai.
- ***Mobil végpontok:*** Működésük nagyban helyzet és kontextusfüggő. Hibás viselkedésük helyzetértelmezési bizonytalanságot okozhat, amely alkalmazási környezettől függően jelentős következménnyel járhat. Az AK7 nyomkövető eszközök alapkategória sorolható ide.
- ***Eseménykritikus végpontok:*** Közvetlen riasztási funkcióval rendelkező vagy közvetlen riasztási eseményt kiváltó eszközök kategóriája. Működésük időérzékeny és rendellenes viselkedésük közvetlen védelmi következménnyel jár. Ilyen eszközök lehetnek a behatolásjelzéshez vagy a tűzjellemzők érzékeléséhez [108] kapcsolódó szenzoregységek. Ide sorolhatók az AK3 szenzorcsomópont és AK5 szenzorinterfész alapkategóriák egyes elmei.

Az ismertetett tipológia független technológiáktól, kommunikációtól és általánosan alkalmazható IoT végpontokra. Ezek a kategóriák még nem a kockázati osztályokat jelölik, hanem előkészítik a következmény súlyosságának meghatározásának alapját.

3.3.2 IoT funkcionális végpont-kockázati osztályok meghatározása

Az IoT funkcionális végpont-kockázati osztályok meghatározásakor nem elegendő figyelembe venni a korábban ismertetett megbízhatósági mutatót, hanem azt is mérlegelni kell, hogy az adott eszköz rendellenes működése milyen következménnyel, hatással jár [109]. A kockázati osztályozás kialakításával az elsődleges célom megmutatni azt, hogy az adott végpont aktuális megbízhatósági állapota és védelmi szerepe együttesen milyen szintű kockázatot hordoz.

A kockázati értelmezéshez két tényezőt vettem figyelembe együttesen: a jelzett esemény vagy kiváltott esemény védelmi következménye és a végpont működésének megbízhatósági bizonytalanság. [20] Ehhez viszont szükséges a megbízhatósági bizonytalanság értelmezése, ami a korábban definiált megbízhatósági indexből vezethető le. Miszerint, minél alacsonyabb a megbízhatósági érték, annál nagyobb a bizonytalanság.

A torzult, időben nem releváns vagy kontextusát vesztő adat ugyanúgy kockázatot jelent, mint a teljes működésképtelenség. Tehát a megbízhatósági bizonytalanságot döntési instabilitásként értelmezem.

A 11. táblázatban látható kockázati mátrix elemei a megbízhatósági bizonytalanság és a védelmi következmény súlyosságának együttes értelmezéséből vannak származtatva. A mátrix úgy értelmezhető, hogy minél nagyobb, súlyosabb egy a végpont által jelzendő esemény következménye, és minél nagyobb az adott végpont működési bizonytalansága, annál magasabb az adott IoT eszköz kockázata és ezzel együtt a meghatározott kockázati osztálya is.

	Bizonytalanság				
Következmény	***Alacsony***	***Mérsékelt***	***Jelentős***	***Magas***	***Extrém***
Kritikus	K3	K3	K4	K4	K4
Súlyos	K2	K3	K3	K4	K4
Jelentős	K1	K2	K3	K3	K4
Mérsékelt	K1	K1	K2	K3	K3
Információs	K1	K1	K1	K2	K3

11. táblázat - Kockázati mátrix

Ez a szemlélet azt eredményezi, hogy azonos funkcionális csoportba sorolható végpontok eltérő kockázati osztályba kerülnek aszerint, hogy milyen az aktuális megbízhatósági állapotuk. Ez fordítva is igaz: azonos megbízhatósági jellemzőkkel rendelkező eszközök alkalmazása magasabb kockázatot eredményez, ha súlyosabb következményekkel járó feladatot látnak el. Mindezek alapján az IoT végpontokat négy kockázati osztályba soroltam.

Az első ilyen kategória az *alacsony kockázatú* IoT végpontok (K1), melyek nem töltenek be közvetlen riasztási feladatot, működésük elsősorban információs jellegű. Az ide sorolható eszközök hibás vagy rendellenes működése nem okoz közvetlen védelmi sérülést, kiesésük vagy késleltetésük rendszerszinten kezelhető, működési bizonytalanságuk nem eredményez azonnali kritikus hatást, és alapfelügyelet mellett üzemeltethetők.

A második kategória a *mérsékelt kockázatú* IoT végpont-kockázati osztály (K2). Ezek a végpontok főként támogató funkciót látnak el, a riasztási döntésekben csak közvetett szerepük van. Időbeli késleltetésük vagy átmeneti kiesésük kis mértékben elfogadható, mivel nem generálnak önállóan döntési eseményt. Rendszerszinten részben kiválthatók, ugyanakkor működésük már befolyásolja a védelmi hatékonyságot.

A harmadik osztály a *közepes kockázatú* IoT végpontok (K3), melyek közvetlenül felelősek riasztási funkcióért vagy védelmi feladatot látnak el, működésük tekintetében időérzékenyek. Az időbeli késleltetés vagy hibás működés hatása jelentős védelmi kockázatot eredményezhet, mivel ez védelmi rést vagy döntési bizonytalanságot okozhat. Rendszerszintű beágyazottságuk és hatásuk jelentős, ezért fokozott felügyeletet igényelnek.

Az utolsó kategória a *magas kockázatú* IoT végpontok (K4), ide tartoznak azok a végpontok, melyek elsődlegesen személy- és vagyonvédelmi feladatot látnak el és közvetlenül befolyásolják a rendszerszintű integritást. Időbeli torzulásuk vagy hibájuk közvetlen biztonsági kockázatot jelenthet, mivel a rendszerszintű döntési folyamat lényeges részét képezik. Rendszerszintű szerepük kulcsfontosságú, ezért strukturálisan kritikus rendszerelemnek minősülnek.

A kockázati osztályok összefoglalva:

- ***K1 – Alacsony kockázatú IoT végpont:***
    - Nem közvetlen riasztási vagy beavatkozási funkciót lát el,
    - Szerepe főként információs,
    - Az időbeli torzulás alacsony hatást fejt ki,
    - Kiesése nem jelent közvetlen és azonnali hatást,
    - Rendszerszinten kiváltható, nem kritikus.
- ***K2 – Mérsékelt kockázatú IoT végpont:***
    - Támogató funkciót lát el,
    - Riasztási döntést nem önállóan generálja,
    - Időbeli késleltetésnek vagy kiesésnek nincs kritikus hatása,
    - Rendszerszinten részben kiváltható.
- ***K3 – Közepes kockázatú IoT végpont:***
    - Közvetlen riasztási vagy védelmi szerepet tölt be,
    - Időbeli torzulás hatása jelentős,
    - Kiesése védelmi kockázatot jelent,
    - Rendszerszintű beágyazottságuk és hatásuk számottevő.
- ***K4 – Magas kockázatú IoT végpont:***
    - Elsődlegesen védelmi funkciót lát el,
    - Időbeli torzulás közvetlen biztonsági kockázatot jelent,

- Rendszerszintű döntési folyamat része,
- Rendszerszintű függőségi láncban betöltött szerepe kulcsfontosságú.

Az ismertetett kockázati osztályozás lehetővé teszi az IoT végpontok strukturált és összehasonlító minősítését funkcionális szerepük és aktuális megbízhatósági állapotuk szerint. A kockázati besorolás dinamikus alkalmazása javasolt, tehát mindig az aktuális állapot és környezethez igazítva, folyamatosan felülvizsgálva. A modell közvetlenül felhasználható tervezési és üzemeltetési döntések támogatására.

3.4 Összegzés, következtetések

Jelen részben ismertettem a 2. fejezetben azonosított jellemző mintázatokra épített biztonságtechnikai relevanciájú fogalmi és megbízhatósági keretrendszert, miszerint az IoT-alapú védelmi rendszert nem pusztán kommunikációs infrastruktúraként, hanem többrétegű modellben definiáltam. A végpontok szerepe elsősorban az események detektálása és az értelmezés magasabb rétegekben valósul meg.

Az IoT végpontok biztonságtechnikai megbízhatóságát, elrugaszkodva a klasszikus műszaki rendelkezésre állástól vagy a kommunikációs jellemzőktől, többdimenziós modellben értelmeztem, ahol a végpontok által szolgáltatott információ döntéstámogató alkalmassága a meghatározó tényező. A modell integrálja a funkcionális (F), időbeli (T), kontextuális (C) és életciklus (L) dimenziókat, kiegészítve a rendszerszintű beágyazottság (S) hatásával. A formalizálás eredménye egy olyan relatív megbízhatósági index, amely 0 és 1 közötti értékkel képes összehasonlíthatóan jellemezni a IoT végpontok személy- és vagyonvédelmi szempontból releváns megbízhatóságát.

A megbízhatósági keretrendszert alapul véve a végberendezések a 2. fejezet alapkategóriájára építve funkcionális szerepükhöz kötött kockázati értelmezését is elvégeztem. Kialakítottam egy kockázati mátrixot, ami alapján négy, K1-K4 funkcionális végponti kockázati osztályt határoztam meg. A besorolás nagyon fontos kiegészítése, hogy a végpont kockázati osztálya nem statikus tulajdonság.

A fejezetben ismertetett eredmények megalapozzák és igazolják az értekezés második hipotézisét (H2). A kapcsolódó kutatási eredményeim lektorált tudományos közleményekben [9][20][70][72][74][84][91][94][96][101][102][103][104][105] jelentek meg, amelyekre nemzetközi hivatkozások is érkeztek.

4 A LORAWAN-ALAPÚ VÉGPONT MEGBÍZHATÓSÁGÁNAK ÉRTELMEZÉSE ÉS ALKALMAZÁSA

A 3. fejezetben ismertetett modell alapján az IoT végpontok megbízhatósága többdimenziós, időben változó paraméterek mentén értelmezhető. A modell lényege az, hogy a végpontok biztonságtechnikai megbízhatósága, de igaz ez rendszerszinten is, nem egyszerűsíthető le csupán kommunikációs, technikai paraméterekre, hanem funkcionális (F), időbeli (T), környezeti (C), életciklus-állapot (L) és a rendszerbe ágyazottság (S) együttes eredményeként és hatásaként jelenik meg.

A személy- és vagyonvédelmi alkalmazások tekintetében a többdimenziós szemlélet kiemelt jelentőségű. Az ilyen rendszerekben a végpont megbízhatósága nagyban befolyásolja a jelzési és riasztási folyamatok működését, az események időben történő felismerését, valamint a szükséges beavatkozások hatékonyságát. Egy IoT-alapú végberendezés instabil működése nem csak technikai szempontból okoz problémát, hanem közvetlen kockázatot jelent a védett objektumokra vagy személyekre nézve. Tehát személy- és vagyonvédelmi rendszerekben ezek az eltérések nem egyszerűen szolgáltatásminőség romlást eredményeznek, hanem valós események detektálásának elmaradásához vezethetnek.

A 3. fejezetben felvázolt modell elméleti kutatások, vizsgálatok alapján és mérések eredményeire építve készült, de szükségesnek látom, hogy valós üzemeltetési környezetben, mérésekkel alátámasztva igazoljam a dimenziók végpontok működésére gyakorolt hatását. Ezért, a jelen fejezet célja a modell validálása különböző mérési eredmények és vizsgálatok értelmezésével. Jelen fejezet a korábban megjelent mérési eredményeimre és elemzéseimre épít, de nem publikáció szerinti bontásban, hanem egységes, összefésült struktúrában feldolgozva. A következőkben ismertetett eredmények beltéri és kültéri környezetben végzett mérésekből, stabilitásvizsgálatból, paraméterérzékeny elemzésekből, speciális esetek teszteléséből, valamint zavarásos kísérletekből származnak LoRa és LoRaWAN kommunikációk alkalmazásával. Az eredmények értelmezése a következő fő kérdések mentén zajlik:

- A kommunikáció stabilitása és sikerességi rátája milyen mértékben függ a környezeti tényezőktől? (Q4.1.)

- A beállítási paraméterek változtatása milyen, nemlineáris hatást gyakorol a működési megbízhatóságra? (Q4.2.)
- A hálózati viselkedés megváltozása hogyan befolyásolja az észlelési és beavatkozási mechanizmusok hatékonyságát? (Q4.3.)
- A megbízhatósági dimenziók elkülöníthetők-e egymástól vagy kimutathatóak kölcsönhatások közöttük? (Q4.4.)
- A végpont életciklus-állapota milyen hatást gyakorol a rendszerre? (Q4.5.)

A fejezet célja egyrészből a többdimenziós megbízhatósági modell gyakorlati validációja, másrészt annak a megalapozása, hogy a végberendezések életciklus-menedzsmentje, különösen a kivonási eljárás, az IoT személy- és vagyonvédelmi rendszerek alapvető elemének kell, hogy legyen.

4.1 Környezeti dimenzió (C) vizsgálata és hatása az időbeli megbízhatóságra (T) és funkcionális dimenzió (F) megjelenése

4.1.1 Budapest belvárosi lefedettségvizsgálat (M1)

A vizsgálatok közül az egyik első mérés egy lefedettségvizsgálat volt, melyet Budapest belvárosában végeztem 2019-ben, olyan helyszínen, ahol a beépítettség kiemelkedően magas. A vizsgálat célja az volt, hogy nagyvárosi környezetben, ahol tégla és vasbeton szerkezetű építmények egyaránt jelen vannak, milyen távolságban és stabilitással valósul meg a kommunikáció. [74]

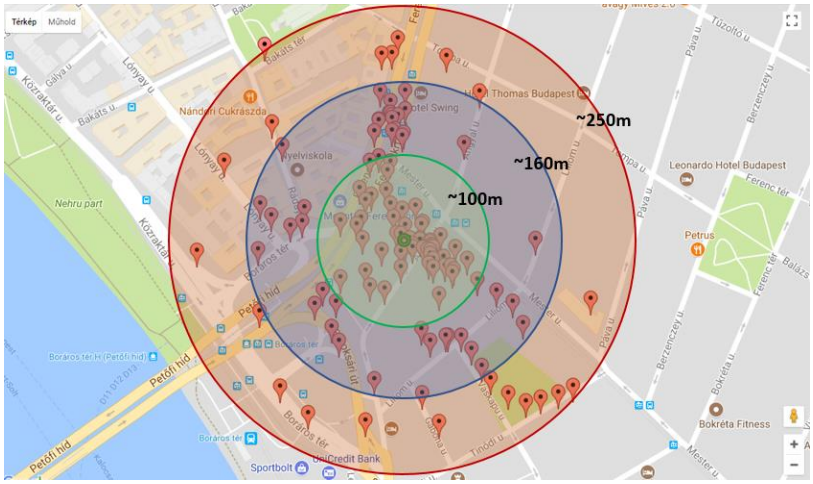
A mérési összeállítás a következő elemeket tartalmazta, amelyet az 5. ábra szemlélteti:

- Végpont: Micromite GPS LoRa MOTE, mely helyadatok küldésére alkalmas.
- Gateway: Kerlink Wirnet iFemtoCell LoRaWAN gateway, mely egy egyszerű, elterjedt beltéri üzemeltetésre készült átjáró.
- Hálózati szolgáltatás: Loriot Network Service, mely biztosítja a hálózati- és szerver szolgáltatásokat.

5. ábra – Budapesten végzett lefedettségvizsgálat mérési összeállítása (Készítette a szerző: [9])

A mérés során alkalmazott LoRaWAN kommunikációs alapparaméterek a következők voltak: DR0, SF12, BW 125 kHz, adatátviteli sebesség 250 bit/s.

A gateway egy többemeletes, tégla társasház lakásában került elhelyezésre. A mérés gyalogosan történt úgy, hogy az átjárótól folyamatosan, koncentrikus körökben (amennyire a közlekedés biztosította) egyre távolabb került a végberendezés, miközben az GPS-koordináták (Global Positioning System: Globális helymeghatározó rendszer) tartalmazó LoRaWAN üzeneteket továbbított. A mérés közben az üzenetek sikeres beérkezése Loriot szolgáltatáson keresztül valósult meg. A pozícióadatok megjelenítéséhez térinformatikai alkalmazást használtam. A mérés eredményét a 6. ábra szemlélteti.



6. ábra - Lefedettségvizsgálat Budapest belvárosában (Készítette a szerző: [74])

Az ábrán a gateway pozícióját a zöld pont jelöli és annak közvetlen környezetében meghatározott zöld, 100 méteres sáv mutatta a legnagyobb továbbítási sikerességi arányt. Ebben a sávban közel 95%-a az elküldött üzeneteknek megérkezett. A következő, kékes terület, ahol a végpont átjárótól való távolsága 100-160 méter között alakult, ott ez a százalékos arány már 70%-ra csökkent. A narancssárgás 160-250 méteres területen az elküldött üzenetek közel fele nem érkezett meg, azaz sikertelen volt az adattovábbítás. Ezt foglalja össze a 12. táblázat.

Távolsági tartomány	**Sikeres adatátviteli arány**	**Értelmezés**
0-100 m	~95%	Magas stabilitás
100-160 m	~70%	Közepes stabilitás
160-250 m	~50%	Csökkent, alacsony stabilitás

12. táblázat - Eredmények alapján elkülönülő területek

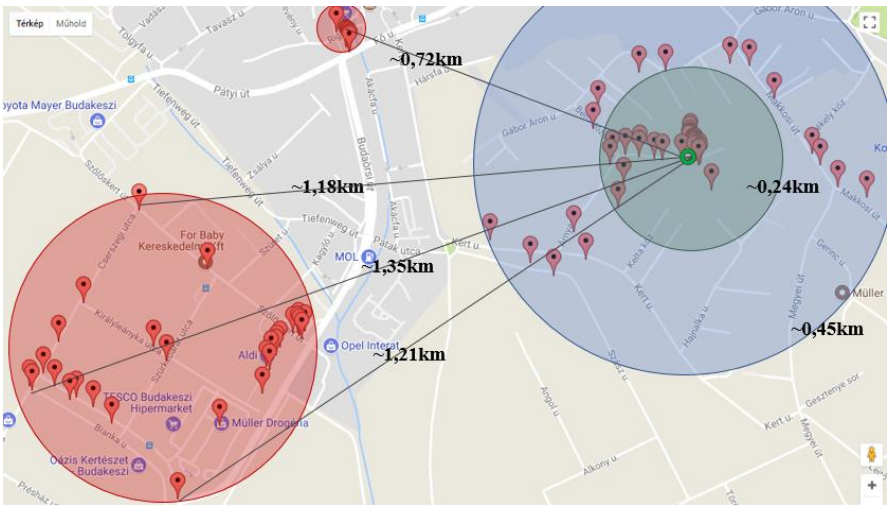
A mérési eredmények alapján a kommunikáció stabilitása nem lineárisan csökken a távolság függvényében, hanem ahogy azt a 6. ábra mutatja, az épített környezet befolyásolja azt. Megállapítható még az is, hogy a sűrűn épített környezet hatása jelentősen érvényesült a vizsgálati helyszínen, ahogy az várható volt.

A mérési eredmények nem csak a kontextuális (C) dimenzió hatását szemléltetik, hanem annak az időbeli (T) megbízhatósági komponensre gyakorolt közvetlen eredményét is. A sikeresen beérkezett üzenetek aránya közvetlenül hatással van arra, hogy a végpont által jelzett esemény a kritikus időablakon belül rendelkezésre áll-e vagy sem.

4.1.2 Budakeszin végzett lefedettségi vizsgálatok (M2)

A második, szintén 2019-ben végzett, mérésnél felhasznált eszközök, mérési összeállítás, kommunikációs paraméterek és a mérési elv megegyezik az előző, budapesti lefedettségvizsgálatéval. A fő különbség a helyszínben van, a méréseket egy Budapest melletti településen, Budakeszin végeztem. A gateway egy erdő melletti, tégla és fa anyagokból épült családiházban került elhelyezésre. A mérés célja szintén lefedettségvizsgálat volt, azaz az adatátviteli távolság és a vételi sikeresség térbeli meghatározása, de más, az imént részletezett környezeti viszonyok mellett. A közeli helyszínek gyalogosan kerültek bejárásra, a távolabbiak pedig személygépkocsival. [74]

A mérés eredményei a 7. ábra szemlélteti, miszerint a zölddel jelölt területen (~240 m távolságig) az elküldött üzenetek közel 90%-os arányban sikeresen megérkeztek, a kommunikáció stabil volt. Ahogy nőtt a távolság, ez az arány jelentősen lecsökkent, a kékkel jelölt 240-450 méteres zónában 60% közeli értékre.



7. ábra - Lefedettségvizsgálat Budakeszin (Készítette a szerző: [74])

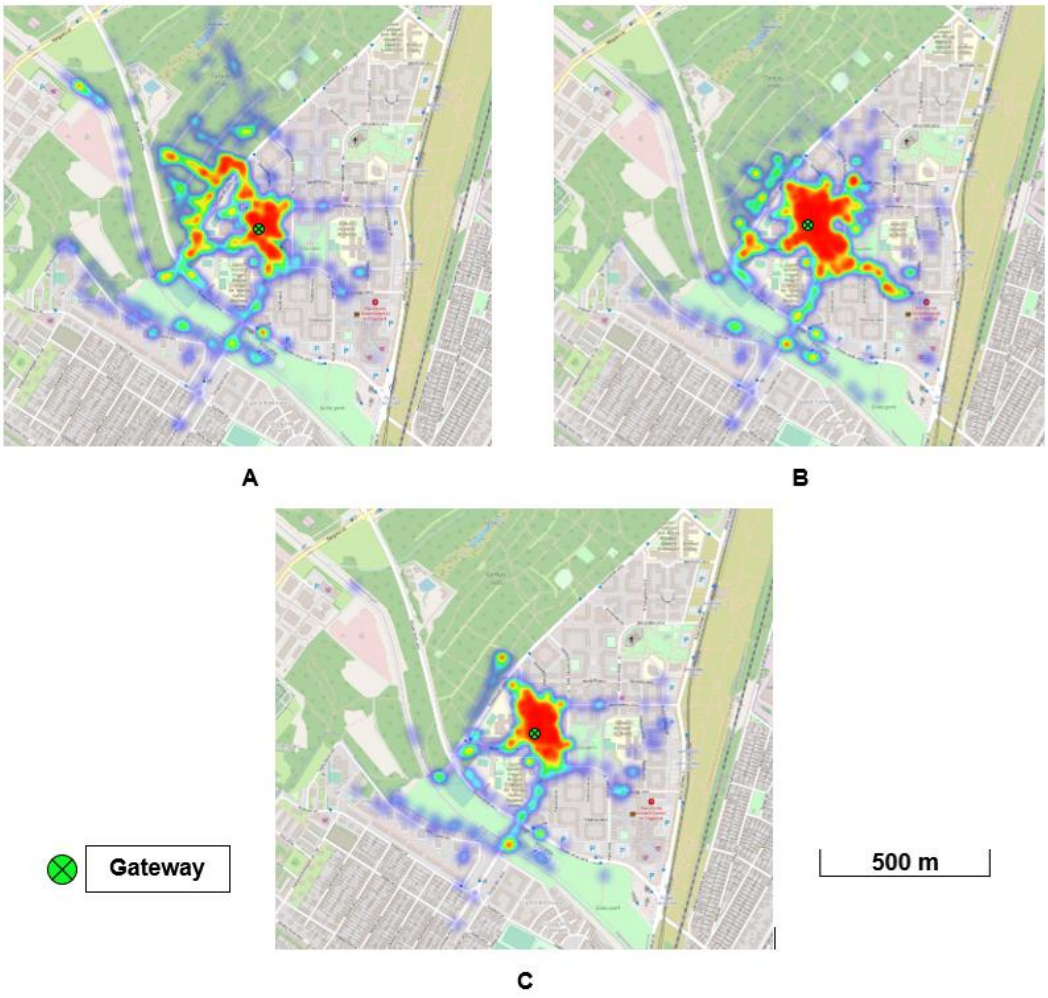
A 7. ábra két pirossal jelölt, elsőre anomáliának tűnő terület, ahol a kommunikáció nem folytonos. Tehát voltak olyan szakaszok, ahol nem valósult meg az adatátvitel, azaz a sikeresen továbbított adatok száma nulla volt. A pirossal jelölt területekről elküldött GPS koordináták 80%-a sikeresen megérkezett. Ebből látszik, például ebben a speciális esetben is, hogy a lefedettség nem kizárólag a távolság függvénye, hanem az aktuális környezeti tényezők is jelentős, nemlineáris hatást fejtenek ki. A Budakeszin végzett mérés jól szemlélteti, hogy azonos eszközkészlet és paraméterezés mellett megjelenő adattovábbítási sikerességi arány térben heterogén, ez alátámasztja a működési környezet (C) meghatározó hatását. Természetesen itt is megjelenik az időbeli (T) dimenzió is, a mérési eredmények mutatják, hogyan befolyásolja a környezet az adatátvitel sikerességét.

4.1.3 Városi lakóparki környezetben végzett több-átjárós mérések (M3)

Az előző két mérés folytatása és kiegészítése egy olyan mérési sorozat elvégzése volt, amelynek megvalósítása vasbeton szerkezetű panelépületek környezetében történt 2021-ben. A mérés célja nem csupán a lefedettségvizsgálat volt, hanem több átjáró párhuzamos működésének összehasonlítása és a végberendezés rádiós paramétereinek elemzése. A mérési elrendezés hasonló az előző két esetben ismertetett kialakításhoz, azzal a különbséggel, hogy az átjáró egy második emeleti panellakás erkélyére került és a Kerlink gateway mellett két másik típus is telepítve lett. A végpont ugyan úgy az aktuális GPS-koordinátákat továbbította és folyamatos mozgásban volt a gatewayek környezetében. [110]

Alkalmazott gateway-ek: kültéri Mikrotik wAP + R11e-LR8 LoRa Gateway modul (A), beltéri Tracknet TBGW10 (B), beltéri Kerlink Wirnet iFemtoCell (C). Az üzeneteket mindhárom gateway egyaránt képes volt fogadni, amely lehetőséget biztosított összehasonlításukra.

A mérés eredményeit a 8. ábra mutatja hőtérképes formában. A piros szín azokat a területeket jelzi, ahol az adott gateway a legtöbb üzenetet tudta fogadni, a sárga-zöld-kék színárnyalatok felé haladva pedig a csökkenő megérkezett üzenetszám látható. A mérési eredmények azt mutatják, hogy a 0-400 méteres tartományban a vasbetonszerkezetekkel zsúfolt terület ellenére a csomagvesztés aránya alacsony. Ahogy nő a távolság, a csomagvesztés aránya is emelkedik és romlanak a rádiós paraméterek. Az ábrán továbbá az is megfigyelhető, hogy ezek a változások szintén nemlineáris formában jelentkeznek, itt is megjelenik a térbeli heterogenitás.



8. ábra - Mikrotik Gateway (A), Tracknet Gateway (B) és Kerlink Gateway (C) hőtérképe (Készítette a szerző: [110])

Ezen a helyszínen elvégzett mérések is jól szemléltetik, hogy a környezeti paraméterek (C) nem izoláltan jelennek meg, hanem az időbeli dimenzióval (T) kölcsönhatásban befolyásolják az IoT végpont személy- és vagyonvédelemben történő alkalmazhatóságát.

4.1.4 Vasbeton szerkezetű mélygarázsban végzett vizsgálat (M4)

Ennek a mérésnek a célja az volt, hogy megvizsgálja, milyen mértékben hat az adatátvitel sikerességére, ha a végberendezés földalatti, vasbeton szerkezetű környezetben kerül elhelyezésre, jelen esetben ez egy mélygarázsban valósult meg. A mérés fókusza itt tehát nem a lefedettség vizsgálatán volt, hanem azon, hogy eltérő adatátviteli sebesség és hasznosadathossz mellett hogyan alakul a sikeres adatátvitel aránya. A méréseket 2019-ben és 2021-ben is elvégeztem, melyek hasonló eredményekkel zárultak. [74][9]

Mérési környezet és konfiguráció a következő volt:

- Végpont: RN2483 alapú saját fejlesztésű eszköz,
- Gateway: Kerlink Wirnet iFemtoCell,
- Hálózati szolgáltatás: Loriot Network Service.

A végpont az imént említett vasbeton mélygarázsba került elhelyezésre, az átjáró ettől a helyszíntől körülbelül 100 méterre kapott helyet egy téglaépület 1. emeletén. Ahogy azt a 13. táblázat mutatja, négy teszteset került kialakításra. A különbség közöttük a hasznos adat hossza, ami 16 és 6 byte volt, illetve az adatátviteli sebesség. Az első 2 teszt esetén nem volt fix beállított adatátviteli sebesség (ADR), a 3. és 4. esetben pedig ez 290-440 bit/s közé volt korlátozva.

Eset	Adatsebesség-korlát	Hasznos adat mérete	Sikeres átvitel aránya
1	290-5470 bit/s (nincs korlát)	16 byte	56%
2	290-5470 bit/s (nincs korlát)	6 byte	80%
3	290-440 bit/s	16 byte	82%
4	290-440 bit/s	6 byte	90%

13. táblázat - Mélygarázsban végzett mérési eredmények (Készítette a szerző: [74][9])

A több órás mérési sorozatok eredménye azt mutatja, hogy alacsonyabb adatátviteli sebesség mellett jelentősen csökken a sikertelen csomagátvitel aránya és a kisebb méretű adatcsomagok továbbítása növelte a sikeresség arányát. A negyedik esetben látszik, hogy ez az érték 90%-ra emelkedett, ami jelentős az első esethez képest, ahol ez 56% volt csupán.

Itt is megjelenik, hogy a kontextuális dimenzió (C) hatással van az időbeli dimenzióra (T), de ezek mellett megjelenik a funkcionális dimenzió (F) is. Bár az adathossz korlátozásával látszólag növelhető a végpont megbízhatósága, de az hatással van a továbbított információ mennyiségére és struktúrájára. Az adatmennyiség csökkentése nem mindig valósítható meg kompromisszumok nélkül, kifejezetten személy- és vagyonvédelmi rendszerekben.

4.1.5 Épületen belül végzett mérések (M5)

Méréseket végeztem beltéren 2020-ban, általános körülmények mellett is egy többemeletes téglaépítésű oktatási épületben, annak a vizsgálatára, hogy a LoRaWAN kommunikáció alternatív megoldás lehet-e olyan esetekben, ahol kisméretű szenzor adatokat kell továbbítani, de Wi-Fi infrastruktúra nem áll rendelkezésre. [105]

A mérések során a hasznos adat hossza 5 byte volt, amely a legtöbb személy- és vagyonvédelmi alkalmazás esetén elegendőnek bizonyul. Az adatátviteli sebességet 980

bit/s értékre választottam, a cél nem a maximális teljesítmény elérése volt, hanem egy valós, energiatakarékos, de robosztus konfiguráció alkalmazása. A mérési összeállítás során saját fejlesztésű RN2483 alapú végberendezést használtam és magyarországi szolgáltatói hálózatot, illetve a Loriot szolgáltatást. Az adatok megjelenítése és feldolgozása sajátfejlesztésű NODE-RED alkalmazással történt. A mérések az érintett épület több helyiségében is elvégzésre kerültek (minden szint folyosója, tantermek, irodák, laborok, műhelyek) és minden érintett helyszínről közel 100%-os, sikeres adattovábbítás valósult meg. Ez igazolja azt, hogy a szolgáltatói hálózat teljes lefedettséget biztosított az egész épületre nézve. Két kiemelt mérés eredményét a 14. táblázat foglalja össze. Az egyik méréssorozat egy gépekkel, asztalokkal teli műhelyben készült, a másik pedig egy számítógépes laboratóriumban. A mérési sorozatból kiemelt részlet 100-100 darab sikeres, kritikus időablakon belül történő, továbbítás részleteit mutatja.

Adatok	**Műhely**	**Laboratórium**
Adatátviteli sebesség	980 bit/s	980 bit/s
Hasznos adat hossza	5 byte	5 byte
Sikeres átvitel aránya	100%	100%
RSSI minimum	-123 dBm	-127 dBm
RSSI maximum	-95 dBm	-103 dBm
RSSI átlag	-111,17 dBm	-117,23 dBm
SNR minimum	-20 dB	-16 dB
SNR maximum	-2,2 dB	-8 dB
SNR átlag	-8,287 dB	-11,93 dB

14. táblázat - Beltéri mérések eredményei (Készítette a szerző: [105])

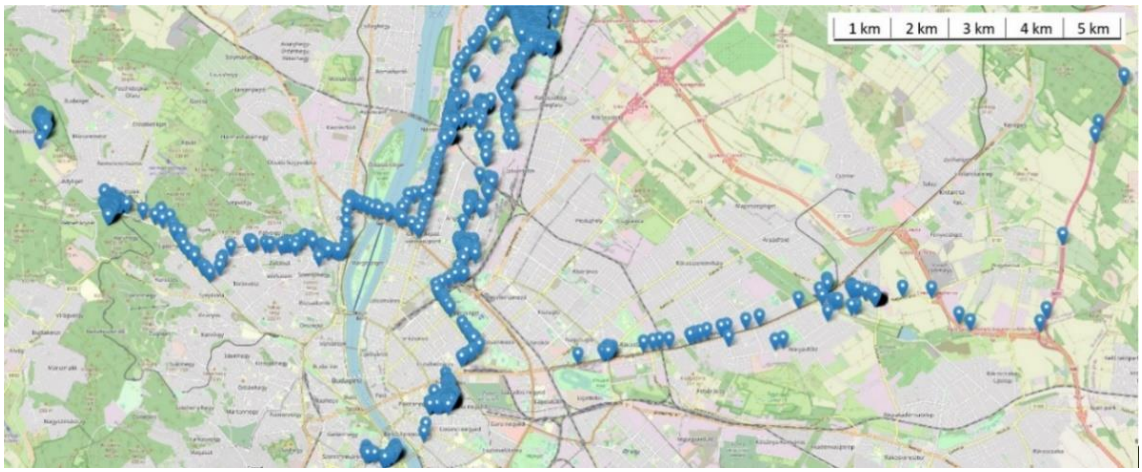
A mérési eredmények azt igazolják, hogy megfelelő környezet (C) és konfiguráció (F) mellett az időbeli tényező (T) értéke közel optimálisnak tekinthető. Bár az RSSI (Received Signal Strength Indicator: Vett jel erősségét jelző mutató) és SNR (Signal-to-noise ratio: Jel-zaj viszony) értékek nem arra utalnak, de az információ továbbítása végig stabil maradt megfelelő konfiguráció mellett. Ez járult hozzá ahhoz, hogy a kommunikáció egy strukturálisan tagolt beltéri környezetben is stabil maradt. Ha funkcionális (F) szempontból vizsgáljuk a mérési esetet, akkor látható, hogy kisméretű, eseményjellegű állapotinformációk kerültek továbbításra, amely a legtöbb személy- és vagyonvédelmi alkalmazás esetén elegendő. Az eredmények megerősítik, hogy a modellben vizsgált dimenziók közötti hatás nem elhanyagolható és nem redukálható le egyetlen paraméterre.

4.2 Szolgáltatói infrastruktúra (S) vizsgálata és hatásai (M6, M7)

Bár az előző beltéri mérés már szolgáltatói hálózaton keresztül történt, de a vizsgálatok főként a környezeti hatások elemzésére fókuszáltak. Ebben az alfejezetben Budapest és környezetében 2020-ban végzett hálózati lefedettségvizsgálati mérések eredményeinek ismertetése történik [101], ahol a fókusz a rendszerbe ágyazottságon (S) belül a hálózati struktúra és annak hatásainak elemzésén van.

A privát LoRaWAN-hálózatok alkalmazása személy-és vagyonvédelmi rendszerekben kontrollált üzemeltetést biztosít, de előfordulhatnak olyan esetek, ahol nem privát infrastruktúra kerül telepítésre, hanem egy lokálisan vagy országos szinten elérhető szolgáltatói hálózat alkalmazása válik gazdasági és üzemeltetés-szervezés szempontjából indokolttá. Magyarországon a legnagyobb kiterjedésű LoRaWAN hálózatot az Antenna Hungária[10] üzemelteti [111], itt végeztem különböző méréseket.

A szolgáltatói hálózati lefedettségvizsgálat célja az volt, hogy megmutassa, hogy a budapesti, kritikus csomópontok mentén milyen hálózati elérhetőség és gateway-redundancia van jelen, illetve a vidéki helyszíneken végzett mérések során a térbeli kiterjedtség és lefedettség vizsgálata.



9. ábra - Budapesten bejárt útvonal (Készítette a szerző: [101])

A mérésekhez GPS-képes adó végpontok kerültek felvételre a szolgáltatói rendszerbe, egy GPS LoRa MOTE, valamint egy ACSIP EK-S76GXB. A beérkezett üzenetek, melyek az aktuális GPS koordinátákat tartalmazták, a szolgáltatói rendszerben létrehozott saját üzemeltetési fiókba érkeztek, melyhez egy alkalmazás került illesztésre az adatok

[10] Jelenlegi neve: 4iG Távközlési Holding Kft.

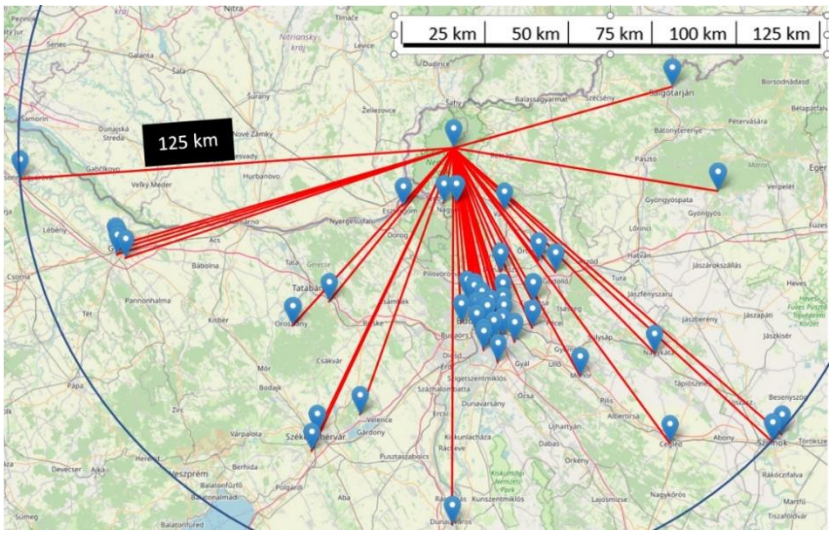
feldolgozásának céljából. Ahogy azt a 9. ábra is mutatja, a budapesti mérési útvonalak kritikus és nagyforgalmú helyszínek mentén vezettek: egyetemi csomópontok, hidak, pályaudvarok és fő közlekedési tengelyek.

A Budapesten végzett mérések (M6) egyik fő eredménye, hogy a szolgáltatói hálózat esetében nem csupán annak van relevanciája, hogy megérkezik-e az üzenet, hanem hogy egy adott helyszínen hány független átjáró képes ugyanazt az üzenetet fogadni. Ez a hálózati redundancia határozza meg a hálózat robusztusságát. [74] A gyalogosan, személygépkocsival és tömegközlekedéssel végig járt helyszínek közül nem volt olyan, ahonnan ne érkezett volna meg üzenet. Viszont különbségek mutatkoztak abban, hogy egy adott üzenetet egyszerre hány átjáró fogadott. A 10. ábra alapján az Árpád híd térségében a végberendezés által 8 gateway volt elérhető. A Hungária körút tengelyén átlagosan 10 gateway fogadta az üzeneteket, de voltak olyan szakaszok, ahol egyszerre 20 darab is. Egy meghatározó híd Budapesten, a Petőfi híd, aminek környezetében átlagosan 5-10 gateway volt elérhető. Az Óbudai Egyetem Tavaszmező utcai kampuszának környezetében a redundancia alacsonyabb volt, átlagosan 2-3 átjáró fogadta az üzeneteket. Budapest belvárosi részén tipikusan 5 gatewayt ért el a végberendezés.

10. ábra - Elérhető gateway-ek az Árpád hídnál (Készítette a szerző: [74])

Az eredmények azt támasztják alá, hogy a szolgáltatói hálózat budapesti lefedettsége összességében stabil, ugyanakkor a gateway-redundancia (S – hálózati struktúra eleme) nem homogén, és erős ingadozást mutathat. Ez személy- és vagyonvédelmi alkalmazásban azt jelenti, hogy ugyanazon végpont különböző telepítési helyein a kommunikáció várható robusztussága eltérő lehet még azonos konfiguráció mellett is.

A mérés kiterjedt a Pest és Nógrád vármegye határán fekvő Csóványos (M7) hegy legmagasabb pontjára is (938 méter), ahol a végpont üzeneteit több nagyvárosi gateway is fogadta, akár több 10 kilométeres távolságból is, ahogy ezt a 11. ábra is szemlélteti. [101]



11. ábra - Mérés Csóványoson (Készítette a szerző: [101])

Ez az eredmény azonban nem tekinthető általános üzemeltetési körülménynek és elvárásnak. Azt viszont inkább demonstrálja, hogy speciális topográfiai és rádiós körülmények mellett a LoRa fizikai réteg kiugró hatótávolságot is produkálhat, ezzel jelezve a terjedési viszonyok nemlinearitását és a környezet domináns hatását.

Mint ahogy az már említésre került, ezek a szolgáltatói lefedettségvizsgálatok nem kizárólag a kontextuális dimenzió (C) hatására koncentrálódnak. A mérések azt szemléltetik, hogy minél nagyobb a gateway-redundancia (S), annál nagyobb a valószínűsége annak, hogy egy lokális árnyékolás vagy egy átjárókiesés hatása áthidalható és nem jelentkezik rendszerszintű problémaként. Emellett, a redundancia közvetlenül kapcsolódik az időbeli megbízhatósághoz (T) is, mivel növeli a vételi ablakon belül megérkező üzenetek arányát.

4.3 Extrém alkalmazási környezetek (C) hatása az időbeli dimenzióra (T) és a konfiguráció szerepe (F)

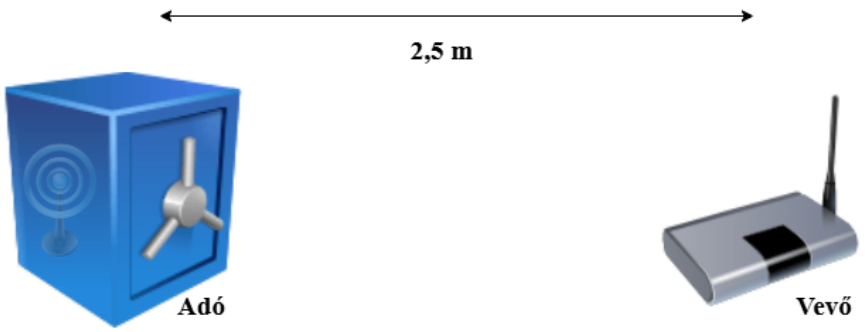
4.3.1 Széfben végzett mérés (M8)

A személy- és vagyonvédelmi alkalmazások esetében nem csak egyszerű kültéri, beltéri, nyílt vagy részben árnyékolt környezetek jelennek meg, hanem szükségessé vállhat a

végpontok extrém fizikai környezetben történő alkalmazása, ahol a legtöbb IoT kommunikáció nem, vagy nagyon korlátozott mértékben működik csak. Ilyen eset, ha egy fémszerkezetű széf belsejébe helyeznek el egy érzékelőt, amely nyitásérzékelési vagy ehhez hasonlatos feladatot lát el.

A 2021-es mérés célja az volt, hogy egy RF szempontból jelentősen árnyékoló környezetben megvizsgálja, hogyan alakul az adatátvitel különböző beállítások mellett és kompenzálható-e a környezeti hatás funkcionális konfigurációk módosításával. [101]

A mérés itt most nem LoRaWAN hálózati struktúrában történt, hanem egy LoRa adó (Nucleo STM32WL55J) és egy LoRa vevő (B-L072-LoRaWAN Discovery board) egységek alkalmazásával, melyeken saját fejlesztésű szoftver futott. Az adó egység a 10 cm falvastagságú, rozsdamentes acél széfbe került elhelyezésre, a vevő egység a széftől 2,5 méteres távolságra, ahogy azt a 12. ábra is mutatja.



12. ábra – Széfmérés mérési összeállítása

A vizsgálatok a széf nyitott és zárt ajtaja mellett is elvégzésre kerültek különböző rádiós paraméterek mellett, ahol az SF értékek folyamatos változtatása történt SF7-SF12 között. Az eredmények összefoglalását a 15. táblázat tartalmazza, ahol a feltűntetett értékek az adott mérési sorozat átlagaira vonatkoznak. A két mérési eset közül a zártajtós a jelentősebb, hiszen az tükröz jobban egy valós alkalmazást.

SF	RSSI nyitott [dBm]	RSSI zárt [dBm]	SNR nyitott [dB]	SNR zárt [dB]	PER nyitott	PER zárt
7	-123,5	-	9,0	-	0%	100%
8	-123,8	-	9,5	-	0%	100%
9	-123,5	-124,5	8,5	9,0	0%	15–20%
10	-124,5	-125,5	8,8	9,5	5%	30%
11	-122,5	-125,0	7,0	9,2	0%	0%
12	-118,0	-125,5	3,0	9,0	0%	0%

15. táblázat - Széfmérés eredményei

Látható, hogy SF7-SF8 beállítások mellett nem lehetett adatátvitelt megvalósítani. SF9-SF10 esetén a PER (Package Error Rate – Csomagvesztés aránya) értéke 20-30% körül alakul, mely szintén jelentős aránynak tekinthető. Viszont, SF11-12 beállítása mellett, amely egyben a legkisebb adatátviteli sebességeket jelenti (250-440 bit/s), az összes adat sikeresen megérkezett.

A mérési eredmények azt mutatják, hogy a környezeti (C) tényező kedvezőtlen (T) hatását, amely jelen esetben egy extrém árnyékolás volt, a megfelelő funkcionális (F) feltételek mellett lehet csökkenteni.

4.3.2 Vízalatti mérés (M9)

Kutatásom alatt egy második extrém környezetben végzett méréssel is foglalkoztam, amely során egy LoRa adóegység természetes állóvízben, a vízfelszín alá került elhelyezésre szintén a 2021-es évben. A mérési konfiguráció megegyezett a széfmérésnél ismertetett konstrukcióval (STM32WL55J adó, B-L072-LoRa vevő). A vizsgálat célja az volt, hogy egy levegőtől jelentősen eltérő fizikai közeg (víz) hatását elemezze a LoRa kommunikáció terjedési viszonyaira, valamint annak konfigurációfüggésére. [101]

A mérés során az adóegység terjedési tényezője folyamatosan változtatásra került SF9-12 tartományban. Az adatküldések azonos paraméterezés mellett 0,45 m és 0,60 m távolságból is elvégzésre kerültek. Referenciaként szabad térben (levegőben) mért csillapítási érték szolgált. Jelen értekezés szempontjából a részletes rádiófrekvenciás számítások nem elsődlegesek; a hangsúly a konfiguráció és a közeg hatásának arányain, trendjein van.

A mérési eredmények összefoglalását a 16. táblázat tartalmazza. Látszik, hogy a levegőhöz képest a víz jelentős többletcsillapítást okoz, ami természetesen várható is volt mindkettő távolság esetében. Megfigyelhető, hogy ahogy csökken az adatátviteli sebesség, azaz az SF érték nő, egyre kisebb mértékű, bár továbbra is jelentős a csillapítás.

Környezet / Konfiguráció	**Csillapítás 0,45 m [dB]**	**Csillapítás 0,60 m [dB]**
Szabad tér (levegő)	24	26
Víz – SF12	34	54
Víz – SF11	51	55
Víz – SF10	34	44
Víz – SF9	47	63

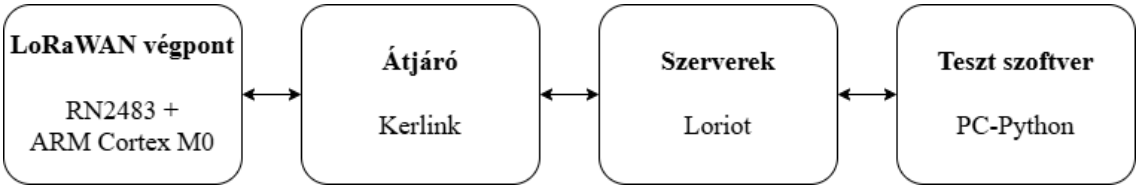
16. táblázat - Vízalatti mérések csillapítási értékei

A víz alatti elhelyezés személy- és vagyonvédelmi IoT végpontok esetében viszonylag ritkán fordul elő, ugyanakkor speciális alkalmazások (pl. víztározók felügyelete, személy vagy objektumkövetés) esetén megjelenhet. A mérés igazolta, hogy a fizikai közeg (C) jelentősen befolyásolja a kommunikációt, ami közvetlen hatással van az időbeli megbízhatóságra (T), ugyanakkor a megfelelő konfigurációválasztás (F), részben képes kompenzálni a kedvezőtlen környezeti hatásokat. Ennek megfelelően a vizsgálat nemcsak egy extrém alkalmazási esetet demonstrált, hanem alátámasztja a többdimenziós megbízhatósági modell érvényességét és a dimenziók közötti kölcsönhatás jelentőségét.

4.3.3 Extrém adatforgalmi aktivitás – nagyméretű adat továbbítása LoRaWAN hálózaton (M10)

Az előzőekben ismertetett mérések esetében főleg kisméretű (~10 byte) adatok továbbítása valósult meg, melyek tipikusan megfelelnek egy személy- és vagyonvédelemben alkalmazott végpontnak. Jelen mérés célja annak az elemzése volt, hogy a LoRaWAN kommunikációt vizsgálja nagyméretű adatállomány továbbítása során, pontosabban digitális képküldés [112] esetében. A mérések a 2023-as évben történtek. [113][70]

A tesztkörnyezet kialakítása során privát hálózatot használtam saját fejlesztésű beágyazott és feldolgozó szoftverrel. A mérési összeállítás négy fő elemből épült fel: LoRaWAN végpont (RN2483 LoRa modul + ARM Cortex M0+ mikrokontroller), Kerlink beltéri gateway, Loriot hálózati és szerverszolgáltatás, PC alapú teszt és feldolgozószoftver (Python), ahogy azt a 13. ábra is szemlélteti.



13. ábra - Képküldés mérési összeállítása (Készítette a szerző: [70])

A továbbított kép mérete közel 63846 byte volt, amely a korábbi mérések megközelítőleg tízezerszerese. Természetesen egyben ezt lehetetlen a kommunikációs korlátok miatt kezelni, így 100 byte-os egységekre osztva, 639 csomagban 10 másodpercenként történt meg az adatküldés. A környezet mezőgazdasági terület volt és a végpont-átjáró közötti távolság nem haladta meg az 1 kilométert.

A vizsgálat során öt eset került implementálásra, melyek eredményét és jellemzőit a 17. táblázat foglalja össze.

Módszer	Kommunikáció iránya	Beépített hibakezelés	Idő	Komplexitás	Hálózati terhelés	Sikerességi arány
1	Uplink	Nem	1 óra 40 perc	1	1	<70%
2	Uplink	Nem	3 óra 20 perc	2	2	<80%
3	Uplink + (Downlink)	Nyugtázás	>= 1 óra 40 perc	3	5	100%
4	Uplink + Downlink	Igen	>= 1 óra 40 perc	4	3	100%
5	Uplink + Downlink	Igen	>= 1 óra 40 perc	5	3	100%

17. táblázat - Képküldési mérések eredményei (Készítette a szerző: [70])

1. módszer: Minden csomag 10 másodpercenként, visszaigazolás és újraküldés nélkül került továbbításra. Ebben az esetben a teljes átvitelhez minimálisan 1 óra 40 perc szükséges, viszont csomagvesztés esetén a kép torzul, hiányos lehet, így a feldolgozás megbízhatatlanná válik. A teljes kép átvitele beépített hibakezelések nélkül csak nagyon ideális esetben valósulhat meg; a mérések folyamán ez csak 70% körüli érték volt.
2. módszer: Minden csomag az előzőekben ismertetett 10 másodpercenként kerül továbbításra, de nem egyszer, hanem kétszer. Ekkor a teljes átvitel ideje duplájára emelkedik (3 óra 20 perc), viszont a sikerességi arány csak kis mértékben növekszik, ezzel együtt pedig emelkedik a hálózati terhelés is.
3. módszer: Ebben az esetben is minden részegység 10 másodpercenként kerül továbbításra, de mindegyikhez tartozik visszaigazolás is, ezáltal a hiányzó csomagok újra küldhetők. Ideális esetben a folyamat 1 óra 40 perc alatt meg tud valósulni, de ha csomagkimaradás van, akkor azok újbóli küldésének idejével ez növekszik. A módszerrel biztosítható a teljes sikeres képtovábbítás, de jelentősen növeli a végberendezés energiafogyasztását és a hálózat terhelését.
4. módszer: Ez a módszer beépített szoftveres hibakezelést tartalmaz a hálózati terhelés csökkentése mellett, de növekvő szoftverkomplexitást eredményezve. 10

másodpercenként kerülnek az üzenetek továbbításra és a feldolgozó oldal detektálja (FCnt alapján) a hiányzó csomagokat, melyeket újból bekér.

5. módszer: Az ötödik megoldás csoportos csomagvesztés-detektáláson alapuló, módosított MPLR-elv (Multi-Packet LoRa: Többcsomagos LoRa kommunikáció) [114] szerint működik. A végpont meghatározott számú (8 vagy annak többszöröse) csomagot küld visszaigazolás nélkül, majd a feldolgozó oldal egy összesített visszajelző üzenetben (bitmaszk formájában) jelzi, hogy az adott csoporton belül mely csomagok nem érkeztek meg. A hiányzó egységek ezt követően célzottan ismét elküldhetők. A magas szoftveres komplexitás és közepes hálózati terhelés mellett biztosítható a sikeres adattovábbítás.

A vizsgálat jól szemlélteti azt, hogy a funkcionális dimenzió (F) radikális megváltoztatása (itt most nem a fizikai környezetre vonatkozóan), jelen esetben nagyméretű hasznosadat továbbítása közvetlen és nem lineáris hatással van további dimenziókra. Az adatátvitel időigénye (T) nagyságrendekkel megnő és megjelenik a rendszerbe ágyazottság dimenziója is (S), hiszen a kétirányú kommunikáció, ismételt küldések jelentősen terhelik a hálózatot.

A mérés azt is alátámasztja, hogy bár LoRaWAN-nal megvalósítható nagyméretű adatok továbbítása (kompromisszumok mellett), azonban ez már nem tartozik a tipikus IoT szenzoralkalmazások közé. Tehát, a funkcionális igény növekedése a megbízhatósági modell több dimenzióját is érintheti.

4.4 Hibás vagy kompromittálódott végpont hatása a hálózat működésére – a rendszer életciklus-dimenziójának (L) vizsgálata (M11)

A személy- és vagyonvédelmi IoT eszközök esetén egy kritikus kérdés, hogy milyen hatása van egy rendellenesen működő, hálózatból részben eltávolított vagy kompromittálódott végpontnak. Jelen alfejezet célja, hogy megvizsgálja azt, hogy egy hibás működést produkáló, hálózati szintű regisztrációból eltávolított eszköznek milyen hatásai vannak az időbeli jellemzőkre, és detektálható-e valahogy ez az állapot statisztikai módszerekkel. A másik cél az életciklus-kezelés aspektusának hatáselemzése.

A mérési vizsgálatra beltéri körülmények között került sor 2025-ben, melyhez Kerlink beltéri gatewayt használtam és 5 végpontot (RN2483 LoRaWAN modul + ARM Cortex M0+ mikrokontroller) saját fejlesztésű szoftverrel. A végberendezések valós

szenzorinformációt továbbítottak a hálózaton külön helyiségekbe elhelyezve. A hálózati adatgyűjtést Loriot szolgáltatáson keresztül valósítottam meg saját fejlesztésű Python feldolgozó programmal. A végpontok minden 10 másodpercben küldtek üzenetet, amely a hálózati késleltetések miatt átlagosan 11 másodperces periódust jelentett. Az eredményekhez a mérési adatokból minden esetben 10-10 órányi adat került feldolgozásra, ami 3200-3300 üzenetet jelentett alkalmanként. A mérések során az elérhető paraméterek közül mindegyik letárolásra került, ezek közül a jelentősebbek: FCnt, RSSI, SNR, ToA[11], DR (SF, BW, CR), csomagok közötti idő, hasznos adat. Ezt az állapotot tekintettem normál működésnek. [104]

A későbbiekben a rendszerhez hozzáillesztésre került egy hatodik eszköz is. Ezt a végberendezést nem regisztráltam a hálózatba, viszont azonos hardverplatformot alkalmaztam, azonos rádiós paraméterekkel. Ami nagy különbség volt az öt normál eszközhöz képest, hogy ez a hatodik folyamatosan, szünet nélkül, egyetlen frekvencián (868,1 MHz) küldte az üzeneteket. [104] Ezt az állapotot tekintem zavart állapotnak [115]; maga a „zavaró” eszköz tekinthető rendellenesen működő végpontnak. Ez a viselkedés megfeleltethető: hibás szoftvernek, rossz konfigurációnak, kompromittált eszköznek vagy szándékos interferenciának.

A kimaradt csomagok detektálásának egyik legegyszerűbb módszere a keretszámláló (FCnt) figyelése, mivel ez egy folyamatosan egyesével növekvő érték, így ettől eltérő esetben csomagvesztés történt. Ismeretében normál és zavart esetre is meghatározható, hogy a vizsgált időszakban hány csomag maradt ki, ennek összefoglalását tartalmazza a 18. táblázat. Látható, hogy a PER normál esetben ~0,5-1,1% közé esik, de a zavart mérések során ez a szám már közel háromszorosa, ~2-4% között alakul. [104]

Eszköz	Normál PER	Zavart PER	PER különbség	Csomagvesztési növekedés [darab]
1	1,01%	2,66%	1,65%	54
2	0,64%	1,99%	1,35%	44
3	1,01%	2,82%	1,81%	59
4	0,55%	2,02%	1,47%	48
5	1,10%	3,83%	2,73%	89

18. táblázat - Csomagvesztések normál és zavart esetben (Készítette a szerző: [104])

Mivel az eltérések, a csomagvesztési arányok relatív kis értékek, ezért Khí-négyzet és Fisher-féle egzakt próbákat is végeztem. Nullhipotézis: A csomagvesztés aránya nem

[11] ToA - Time on Air: Levegőben töltött idő (adásidő).

függ attól, hogy van-e zavarás. Ezek rendkívül alacsony p-értéket adtak ($<10^{-6}$), amely statisztikailag bizonyítja, hogy a csomagvesztési arány növekedése nem véletlenszerű ingadozás, hanem a zavaró eszköz jelenlétével összefüggő hatás.

Az RSSI és SNR paraméterek vizsgálata nem mutatott jelentős, egységes, rendszerszintű eltolódást a normál és zavart állapot között. Az SNR átlagérték változása minden eszköznél minimális tartományban maradt, műszaki szempontból nem volt releváns. Az RSSI esetében ugyan egyes eszközöknél megfigyelhető eltolódás megjelent, azonban annak iránya nem volt egységes, így nem tekintettem a zavarás megbízható indikátorának. Erről ezért nem tartom szükségesnek összehasonlító táblázat vagy ábra beillesztését. Tehát összefoglalva, az RSSI és SNR értékek eltérése (nem változtak jelentősen) nem utalt rendellenességre az előző PER alapú vizsgálattal ellentétben.

A csomagok közötti időintervallumokat is vizsgáltam, összehasonlítva az alapvető statisztikai mutatókat a normál és zavart mérések során. Ennek összefoglalását tartalmazza a 19. táblázat.

	Normál					**Zavart**				
Eszköz	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
Átlag [s]	11,023	11,032	11,030	11,032	11,032	11,024	11,033	11,025	11,033	11,033
Min. [s]	10,957	10,956	10,974	10,820	10,976	10,947	10,995	10,940	10,970	10,998
Max. [s]	11,089	11,115	11,085	11,243	11,098	13,104	13,107	13,091	13,086	13,090
Szórás [s]	0,010	0,011	0,011	0,013	0,011	0,039	0,039	0,039	0,038	0,039
Medián [s]	11,021	11,037	11,034	11,037	11,037	11,021	11,037	11,021	11,036	11,037

19. táblázat - Csomagok közötti időintervallum statisztikai vizsgálata (Készítette a szerző: [104])

Az átlag és a medián esetében elhanyagolható mértékű különbség mutatkozott, a változás 0,001-0,005 s nagyságrenden belül maradt. A minimum értékek is stabilitást mutattak, a ~10,94-10,99 s tartományon belül mozogtak. Jelentős eltérések a maximális értékek és a szórás esetén jelentkeztek. Normál esetben a maximális időintervallum alig több 11 másodpercnél, de zavart esetben ez 13 másodperc fölé is emelkedett. Ez összességében arra utal, hogy ritka, de jelentős mértékű időbeli kilengések jelentek meg. A szórásnál látható változás, hogy 0,01-0,013 másodpercről 0,039 másodpercre emelkedett, jelzi, hogy a kommunikáció időbeli stabilitása romlott, annak ellenére, hogy az átlagos periódusidő változatlan maradt.

A méréseket a megbízhatósági dimenziómodell alapján a következőképpen lehet értelmezni. A rádiós közeg (C) degradálódott egy hibás működésű eszköz miatt. A csomagvesztés aránya nőtt és a csomagok közötti idő (T) is. Az öt végpont esetében eltérő

hatás érvényesült, ez a rendszer heterogén viselkedésére és a hálózati topológia szerepére utal (S). A rendellenesen működő eszköz, bár nem azonos mértékben, de negatív hatással volt minden végpontra. Ez igazolja azt, hogy egy hibás vagy kompromittált eszköz jelenléte (L) a rendszerben nem izolált problémát okoz, hanem hatással van a többi szereplőre és a megbízhatóság további dimenzióira.

4.5 Összegzés, következtetések

A fejezetben ismertetett 2019-2025 közötti intervallumban végzett mérések és azok eredményei együttesen igazolják, hogy a LoRaWAN végpontok megbízhatósága, nem fejezhető ki megfelelően megválasztott rádiós paraméterekkel vagy magával a teljes lefedettséget biztosító környezettel. A mérések során értelmezett dimenziókat a 20. táblázat foglalja össze.

Mérés	**C**	**T**	**F**	**S**	**L**
M1	✓	✓	(✓)	-	-
M2	✓	✓	(✓)	-	-
M3	✓	✓	(✓)	✓	-
M4	✓	✓	✓	-	-
M5	✓	✓	✓	✓	✓
M6	(✓)	✓	-	✓✓	-
M7	✓	(✓)	-	✓	-
M8	✓✓	✓	✓✓	-	-
M9	✓✓	✓	✓	-	-
M10	-	✓✓	✓✓	✓	-
M11	✓	✓✓	(✓)	✓	✓✓
Jelölés: ✓ = érinti, ✓✓ = elsődleges fókusz, (✓) = másodlagosan / implicit módon megjelenik, - = nem vizsgált/nem jelenik meg					

20. táblázat - Mérések és dimenzióik összefoglalása

A vizsgálatok következetesen alátámasztják, hogy a kontextuális paraméterek (C) térben heterogén, nemlineáris hatást fejtenek ki a kommunikáció stabilitására, ami közvetlenül megjelenik az időbeli dimenzióban is (T). Ezt jól mutatja a sikeresen beérkezett csomagok aránya. A belvárosi és budakeszi lefedettségi vizsgálatok, valamint a panelkörnyezetben végzett több-átjárós mérések egyaránt azt mutatják, hogy a továbbított események vagy szenzoradatok detektálás időszerűsége nem a távolság egyértelmű függvénye, hanem a lokális hatások érvényesülésének, az épületszerkezeti befolyások és a topológiai sajátosságok kombinációjának eredője.

A mérések második központi eredménye, hogy a kedvezőtlen környezeti hatások (C) részben kompenzálhatók megfelelő funkcionális konfigurációval (F), de nem bármilyen

mértékben, hanem korlátokkal és kompromisszumokkal csak. A vasbeton mélygarázsban végzett mérések során a hasznos adat és az adatátviteli sebesség korlátozása számottevő mértékben növelte a sikeres továbbítási arányt, de személy- és vagyonvédelmi alkalmazások tekintetében ezek a korlátozások nem minden alkalmazás esetén valósíthatók meg komoly kompromisszumok nélkül. Hasonló eredmények születtek az extrém környezetekben (széf, víz alatti, képküldési) végzett mérések során is, ahol a fizikai közeg jelentősen befolyásolta a terjedési feltételeket. Tehát a fejezet rámutatott arra, hogy a funkcionális dimenzió kompenzációs elemként jelenik meg, paraméterezési döntések eredményeként.

A szolgáltatói gateway-hálózaton végzett mérések behozták a koncepcióba a rendszerbe ágyazottság (S) kérdéskörét, ahol a gateway-redundancia és a hálózati struktúra szerepe jelent meg. A budapesti útvonalakon végzett mérések megmutatták az elérhető szolgáltatói gateway-ek számán keresztül, hogy ugyanaz a végpont azonos konfigurációval más viselkedést mutathat a topológiai redundancia miatt. Ha nagyobb a redundancia, akkor egy lokális árnyékolás, fizikai környezeti eltérés vagy átjárókiesés hatása sikeresebben áthidalható, ami személy- és vagyonvédelmi alkalmazások tekintetében azt eredményezi, hogy az üzenetek nagyobb valószínűséggel érkeznek meg a kritikus időablakon belül.

A fejezet utolsó részének konklúziója, hogy a megbízhatósági modell időben változó jellege és az életciklus-dimenzió (L) hatása nem elhanyagolható. A normál/zavart beltéri környezetben elvégzett mérések modellezték egy lehetséges hatását egy rendellenesen működő vagy kompromittált eszköznek. Az eredmények alapján, a csomagvesztések száma megemelkedett, a késleltetésekben ritka, de nagyobb mértékű kilengések jelentek meg. Ez azt jelenti, hogy szükség van az életciklus-menedzsment teljes sorára. A fejezet megalapozta azt, hogy a kivonási eljárás nem egy adminisztratív szükségesség, hanem a megbízhatóság fenntartásának egyik gyakorlati eszköze.

Mérési eredményeimmel igazoltam, hogy a kontextuális környezet (elhelyezés, fizikai struktúra, közeg, környezeti paraméterek) meghatározó és nemlineáris hatással vannak a LoRaWAN végpontok személy- és vagyonvédelmi alkalmazhatóság szempontjából releváns időbeli mutatóira. Kimutattam, hogy a funkcionális paraméterezés átstrukturálásával a környezeti hatások részben kompenzálhatók, azonban ez időbeli, erőforrásbeli kompromisszumokat követel, amelyek személy- és vagyonvédelmi

rendszerekben tervezési és alkalmazási korlátként jelennek meg. Méréseken alapuló, a kommunikációs jellemzőkön túlmutató, statisztikai módszerekkel igazoltam, hogy egy rendellenes végpont-állapot jelentősen torzítja az értékelést. A fejezetben bemutatott eredmények alapján bizonyítottam az értekezésben megfogalmazott harmadik hipotézist (H3); az igazolás alapjául szolgáló kutatási eredmények lektorált tudományos publikációkban [9][70][74][101][104][105][110][113] kerültek közlésre, amelyekre több nemzetközi hivatkozás is érkezett.

5 ESZKÖZ-ÉLETCIKLUS ÉS KIVONÁSI ELJÁRÁS

Az elvégzett vizsgálataim és kutatómunkám során azt tapasztaltam, hogy a fő fókusz az IoT végpontok telepítésére és üzemeltetésére korlátozódik. Technológiai szempontból a kommunikációs specifikációk, szabványok részletesen taglalják az eszközök aktiválási mechanizmusait, kulcskezelését vagy akár a jogosultságkezelését is, amely az életciklus-menedzsment egy részét fedi csak le. Az adott eszköz hálózatból történő kivonása nem jelenik meg kellő hangsúllyal vagy gyakran alulreprezentált.

Az IoT eszközök életciklus-dimenziója nem redukálható le csupán a telepítési és üzemeltetési fázisokra. [107] Az ISO/IEC 30141-ben felvázolt IoT referenciaarchitektúra értelmezése szerint, az eszközök kivonása is az életciklus szerves részét képezi. Amennyiben a kivonás nem történik meg megfelelően, úgy a rendszerben maradó eszköz rejtett kockázatot jelent. Hasonló elvek jelennek meg a ISO/IEC 27002-ben [116] és az ETSI EN 303 645-ben [27] is, miszerint a hozzáférési jogosultságok megszüntetése és a megfelelő kulcskezelés, visszavonás is a folyamat része kell, hogy legyen. Bár az egész procedúra egy adminisztrációs lépéssorozatnak tűnik, de az IoT-eszközök kivonása nem csupán ennyit jelent, hanem a rendszer biztonsági állapotának strukturált módosítását eredményezi. A nem megfelelő életciklus-lezárás számos rejtett kockázatot jelenthet [117][118][119], amelyet a fejezet további részeiben részletesen kifejtek.

A probléma fontossága jól szemléltethető olyan IoT rendszerek esetében, ahol az eszközök dinamikus telepítése és cseréje alapvető jelenség. Az értekezésben a LoRaWAN alapú eszközöket használom fel reprezentatív példának, miszerint az eszközök hálózatból való ellenőrzött kivonása nem jelenik meg protokoll szerinti, formalizált módszerként, amely az életciklus-kezelés alapvető hiányosságát eredményezi.

A jelen fejezet célja ismertetni azt, hogy az eszközök-életciklusának lezárása az IoT személy- és vagyonvédelmi rendszerek szerves részét kell, hogy képezze és biztonságtechnikai szempontból kiemelt jelentőségű. A fejezet további részeiben az életciklus szakaszait, de kiemelten a kivonási eljárást, védelmi nézőpontból mutatom be és a LoRaWAN technológia példáján szemléltetem. Az értekezés a kivonás tárgyalása során a leszerelt eszközök hulladékgazdálkodási, újrahasznosíthatósági, környezetvédelmi kérdéseit nem vizsgálja és az információbiztonsági szempontokkal csak a szükséges mélységben foglalkozik.

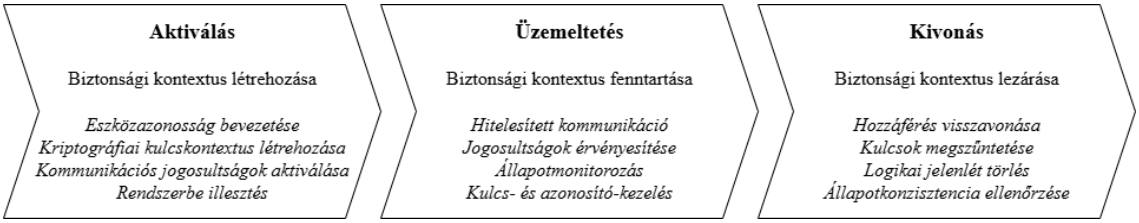
A 3. és 4. fejezet eredményeit felhasználva jelen fejezet a következő kutatási kérdésekre keresi a választ:

- Elegendő-e az IoT-végpont kivonására csupán üzemeltetési-adminisztratív műveletként tekinteni, ha az eszköz fizikai és logikai jelenléte szétválik? (Q5.1.)
- Milyen inkonzisztens állapot jöhet létre az eszköz logikai és fizikai szétválásakor és ennek nem megfelelő kezelése milyen következményekkel jár? (Q5.2.)
- Milyen rejtett védelmi kockázatot okoz, ha a végberendezés életciklus-lezárása nem történik meg formalizált módon, és ennek milyen torzító hatása van az állapotértékelésre? (Q5.3)
- Milyen követelményeknek kell érvényesülnie egy IoT-végpont kivonása során, hogy az konzisztens, reprodukálható és auditálható legyen? (Q5.4)
- Milyen lépésekben valósítható meg a LoRaWAN végberendezések kivonási eljárása és ez milyen összhangban van azok specifikációjával? (Q5.5)

A fejezet célja annak az igazolása, hogy az IoT-végpontok kivonása nem egy elhanyagolható melléktevékenység, hanem a rendszer állapotára közvetlen hatást gyakorló beavatkozás. A fejezetben olyan modellek és keretrendszer kerül ismertetésre, amely IoT környezetben, de kifejezetten LoRaWAN végberendezések kivonására optimalizált, biztosítva a konzisztens, ellenőrizhető fizikai és logikai lezárást.

5.1 Az IoT-eszközök életciklusának szakaszai biztonságtechnikai aspektusból

Az IoT eszközök életciklusának szakaszai általánosan három fázisra bonthatók: telepítés (aktiválás), üzemeltetés és kivonás. [27][120][121] Ezek az életciklus állapotok vagy menedzsment folyamatok egymás utáni lépések sorozataként írhatóak le, ahogy azt a 14. ábra is szemlélteti. Azonban azt meg kell jegyezni, hogy ezek eltérő kockázati profilt reprezentálnak.



14. ábra - IoT eszközök életciklus-modellje

A telepítés fázisa alatt itt nem a klasszikus szerelési munkálatokat értem, bár az is a folyamat része, hanem IoT szempontból az aktiválás lépéseit, ahol az eszköz kriptográfiai és logikai identitása beillesztésre kerül a rendszerbe, ez felel meg a kontextus kialakításának. A második szakasz az üzemeltetés, ahol az identitás aktív, hitelesített és megfelelő jogosultságokkal rendelkezik. A kivonás, az utolsó életciklus-menedzsment elem nem csupán a működés megszüntetését jelenti (például eszköz leszerelése), hanem a korábban létrehozott kontextus lezárását minden szempontból.

Védelmi nézőpontból az életciklus-állapot vizsgálata a következő kérdések mentén értelmezhető:

- Érvényes-e még a kialakított kontextus?
- Érvényes-e még a hitelesítési, kriptográfiai kulcskészlet?
- Jogosult-e az eszköz hálózati kommunikáció folytatására?
- Szerepel-e az adott eszköz a rendszernyilvántartásban?
- Megfelel-e egymásnak az eszköz fizikai és logikai állapota?

Ha az életciklus zárása nem történik meg strukturált, ellenőrzött módon, akkor ezen kérdések válaszai inkonzisztensé válhatnak. Ha egy eszközt fizikailag eltávolítanak, attól még logikailag hitelesített entitásként jelenhet meg a rendszerben a megfelelő kivonási lépések elvégzésének hiányában. Ha ez nem is azonnal jelentkezik rendszerszintű problémaként, de növeli a kockázatot és torzítja az állapotértékelést.

Mivel a kivonási eljárás az IoT eszközök életciklusának szerves része és az értekezés is ezen kérdéskörrel foglalkozik a továbbiakban, így fontosnak látom részletesebben összefoglalni, hogy mit is jelent ez. A kivonási eljárást egy olyan folyamatnak tekintem, amelyet az IoT-eszköz életciklusának záró fázisában hajtanak végre strukturált és kontrollált módon, annak érdekében, hogy az adott végpont hálózati, logikai és kriptográfiai jelenlétét megszüntessék. [72] A kivonási eljárás részben tekinthető az aktiválási folyamat fordítottjának, de nem egyértelmű inverze, azaz amíg az aktiválási folyamat általában protokollszinten, specifikáció szintjén jól azonosítható módon megjelenik, addig a kivonási folyamat a legtöbb esetben implementációs vagy üzemeltetési kérdés marad.

Összességében megállapítható, hogy az IoT eszközök kezelése nem ér véget az üzembe helyezéssel és üzemeltetéssel, hanem magába kell foglalnia az eszköz szabályozott eltávolítását is, amelynek hiánya védelmi kockázatot jelent és csökkenti az eszköz

megbízhatósági indexét, ezzel növelve a megbízhatósági bizonytalanságát és a kockázati osztályát (*lásd: 3. fejezet*).

5.2 Rejtett védelmi kockázatok az eszköz-életciklus során

5.2.1 A kivonási eljárás szükségességének tipikus esetei

Kivonási eljárásra nem feltétlenül csak valami rendkívüli esetben van szükség, hanem az IoT eszközök tekintetében ez az életciklusuk természetes része. Az eljárás szükségessége több, egymástól eltérő esetben válhat jelentőssé.

Az első ilyen alapeset a *funkcionális okból történő kivonás*, amikor az adott eszközre a továbbiakban nincs szükség a rendszerben. Ez akkor fordul elő, ha például egy rendszer lezárása történik, a rendszert átalakítják, az eszközt lecseréik vagy átszervezés történik. [118] Ez elsősorban üzemeltetési érintettségű, de ugyanúgy igényli a megfelelő lezárást.

A második alapeset a *meghibásodás vagy fizikai sérülés*. [85] Ez az eszközök életének természetes velejárója, hogy valami műszaki hiba miatt működésképtelenné válik fizikailag, feladatát nem tudja betölteni, ezért elérhetetlen lesz a rendszer szempontjából vagy fizikailag eltávolítják. Ekkor a fizikai és logikai állapot szétválik és a rendszerszinten érvényes kontextus még fennmaradhat.

A harmadik eset, ha az adott IoT végpont *kompromittálódott vagy biztonsági incidens történt*. [122][107] Ha felmerül a gyanúja például, hogy kulcsszivárgás vagy jogosulatlan hozzáférés, módosítás történt vagy az eszköz anomáliára utaló viselkedést produkál, akkor feltétlenük szükséges a megfelelő kivonási eljárás lefolytatása, hiszen már nem csak üzemeltetési kérdésként jelenik meg, hanem az incidenskezelés egyik eszközeként.

A negyedik alapeset, amikor *változás történik az eszköz konfigurációjában vagy szerepkörében*. Előfordulnak olyan helyzetek, amikor az IoT-végpont új funkciót kap, másik rendszerbe kerül vagy megváltozik a szerepköre. [123] Ekkor szükségessé válhat a korábbi kontextus lezárása és az új kontextus létrehozása, különösen, ha az azonosítókban, kulcsokban változás történt.

A négy esetben az a közös, hogy az adott IoT eszköz fizikai vagy funkcionális szerepe szűnik meg vagy szükséges azt megszűntetni, de ha nincs megfelelően strukturált és ellenőrzött kivonási eljárás lefolytatva, akkor kontextusuk fennmaradhat, melyek rejtett védelmi kockázatokat okozhatnak. A következőkben e kockázatokat elemzem.

5.2.2 Rejtett védelmi kockázatok

Az előző részfejezet összefoglalta, hogy milyen esetekben van szükség kivonási eljárásra és több esetben is kiemelésre került a rejtett védelmi kockázat kérdésköre. Az IoT eszközök életciklusának lezárása során a legnagyobb problémát nem az azonnali hibák okozzák, hanem az inkonzisztens állapot kialakulása jelenti.

Az első ilyen kockázat a *„láthatatlan" vagy „szellem" eszközök* jelenléte. Ez akkor fordul elő, ha az adott eszköz már fizikailag nincs jelen a rendszerben, de azonosítói, kulcsai továbbra is érvényben vannak [124], érvényes a hitelesítési és jogosultsági kontextusa formálisan. Ez rendszerszinten torzíthatja az állapotképet, lehetőséget biztosíthat jogosulatlan ismételt használatra vagy egyéb visszaélésekre.

A második ilyen eset a *jogosulatlan jelenlét*. Amennyiben a hitelesítéshez szükséges adatok és a kriptográfiai kulcsok továbbra is aktívak maradnak egy olyan eszköz esetében, amely már nem képezi (vagy nem kellene, hogy képezze) a rendszer részét, akkor az eszköz vagy annak klónja [121] továbbra is képes lehet a hálózaton történő működésre.

A harmadik rejtett kockázat a *hamis biztonságérzet* [11] fennállása. Ha az eszközhöz tartozó minden adat törlésre kerül a menedzsment-felületi oldalról, az eszköz lezárt állapotúnak tűnhet, de közben pedig a tényleges aktív kontextus fennmaradhat, ha a kivonás nem determinisztikusan történt.

A negyedik rejtett kockázat a *kulcs- és hozzáféréskezelési inkonzisztencia*. Az IoT-végpontok általában több rétegben folytatnak hitelesítési mechanizmusokat és ezekben a szintekben eltérő módszerek alkalmazására lehet szükség. [107] Különösen igaz ez nagykiterjedésű, folyamatosan változó rendszerek esetében.

Az azonosított rejtett kockázatok összességében arra utalnak, hogy az életciklus zárásának hiánya vagy hiányossága általában nem egyszerű működési hibák okozója, az adott eszköz, de akár a rendszer hosszútávú megbízhatóságát és egységét befolyásolják.

5.3 Módszertani követelmények a kivonási eljárással szemben

A kivonási eljárás lépéseinek meghatározása előtt fontosnak tartom összefoglalni, hogy milyen módszertani követelményeknek [125][126][127] kell megfelelnie. Az IoT rendszerekkel kapcsolatos vagy kapcsolatba hozható architekturális és

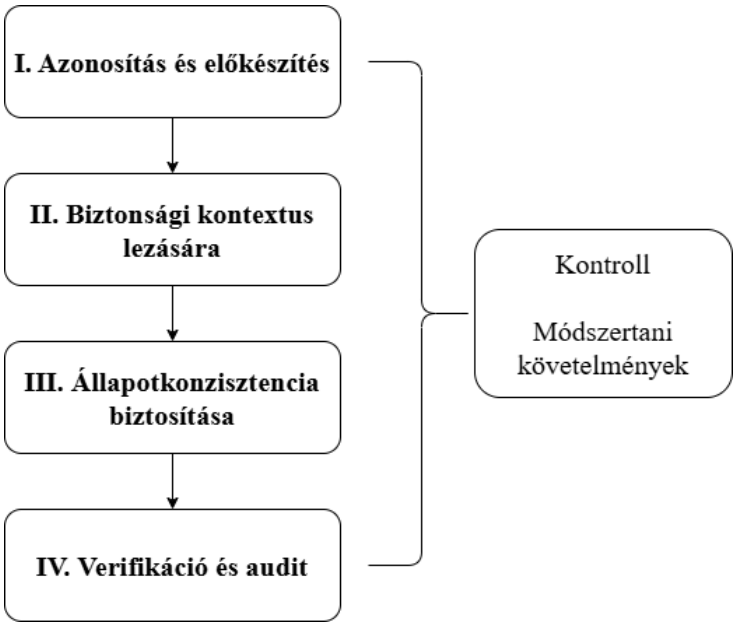
információbiztonsági szabványok kiindulópontot biztosítanak ehhez. A követelményeket a következőkben határoztam meg:

- ***Determinisztikusság***: a kivonási eljárás lépéseinek egyértelműen definiáltnak kell lennie és biztosítani kell azok reprodukálhatóságát. A folyamat minden lépésének előre meghatározott feltételek szerint kell történnie egyértelmű kimeneti állapotokkal.
- ***Visszaellenőrizhetőség és auditálhatóság***: A kivonási eljárásnak végig dokumentáltnak és visszaellenőrizhetőnek kell lennie, a naplózás és az elszámolhatóság kiemelten fontos. Az állapotváltozásokat és azok idejét rögzíteni szükséges, az érintett komponenseket azonosítani-, a felmerülő hibákat és kivételeket rögzíteni kell, az elvégzett jogosultság- és kulcsmegszüntetések igazolása szintén elvárás.
- ***Állapot egyértelműsítése***: A kivonás elvégzését követően az eszköz állapota nem lehet bizonytalan. Egyértelműen jegyezni kell, hogy a végpont rendelkezik-e hozzáféréssel vagy sem, a következő állapotok egyikét kell hozzárendelni: aktív, kivonás alatt, deaktivált.
- ***Kriptográfiai kontextus teljes lezárása***: A kivonás nem korlátozódhat csupán az adminisztratív törlésre, hanem biztosítani kell a hitelesítési adatok, kulcsok, egyéb azonosítók megszüntetését. Az eljárás során ellenőrizni kell, hogy az érvényes hitelesítési kulcsok, azonosítók visszavonásra kerüljenek és a kommunikációs jogosultság megszűntetését. Biztosítani kell az eszköz további hálózati jelenlétének kizárását.
- ***Hálózati terhelés minimalizálása***: A kivonási eljárás során fontos, hogy ne jelentkezzen aránytalanul nagy hálózati terhelés, amely a működést vagy a funkcionalitást befolyásolja. Figyelmet kell fordítani az arányosságra és az optimalizálásra.
- ***Többrétegű állapotkonzisztencia***: Mivel az IoT rendszerek többrétegű architektúrával rendelkeznek, ezért az eltérő rétegek kezelése során fenn kell tartani a következetességet.

Az ismertetett módszertani követelmények alapján a kivonási eljárás csak akkor tekinthető megfelelőnek, ha formalizált, determinisztikus és auditálható módon biztosítja az eszköz biztonsági kontextusának teljes és konzisztens lezárását.

5.4 IoT-végpont életciklus-lezárási modell

Az előző alfejezet módszertani követelményeit figyelembe véve megalkotható egy olyan életciklus-lezárási modell, amely nem határozza meg az adott IoT-végpont implementációs részleteit, nem megy bele a technikai és kommunikációs sajátosságokba, hanem általános keretet definiál a procedúrához és alapot szolgáltat későbbiekben konkrét specifikációra történő alkalmazásra. A modellt 4 fázisból építettem fel, amelyet a 15. ábra foglal össze.



15. ábra - IoT-végpont életciklus lezárási modell

Az első lépés az *azonosítás és a kivonás előkészítése*, ahol az érintett eszköz egyértelmű identifikációja történik és az aktuális állapotának felmérése. Ehhez a fázishoz tartozik az eszköz egyedi azonosítójának meghatározása, a kommunikációs jogosultságának állapotfelmérése, a kivonásban érintett további rendszerkomponensek azonosítása és a kivonás indokának rögzítése. Így biztosítható, hogy a kivonás megkezdése indokolt döntés alapján, dokumentált és egyértelmű módon történjen.

A második lépés a *biztonsági kontextus lezárása*, melynek célja az adott IoT-végpont kriptográfiai kontextusának megszüntetése. Itt kell végrehajtani a kommunikációs jogosultság visszavonását, a kapcsolódó azonosítók, kulcsok, tokenek érvénytelenítését, lehetőség szerint a végberendezés értesítését a hálózati működés beszüntetéséről és az eszköz teljes kizárását a hálózatból.

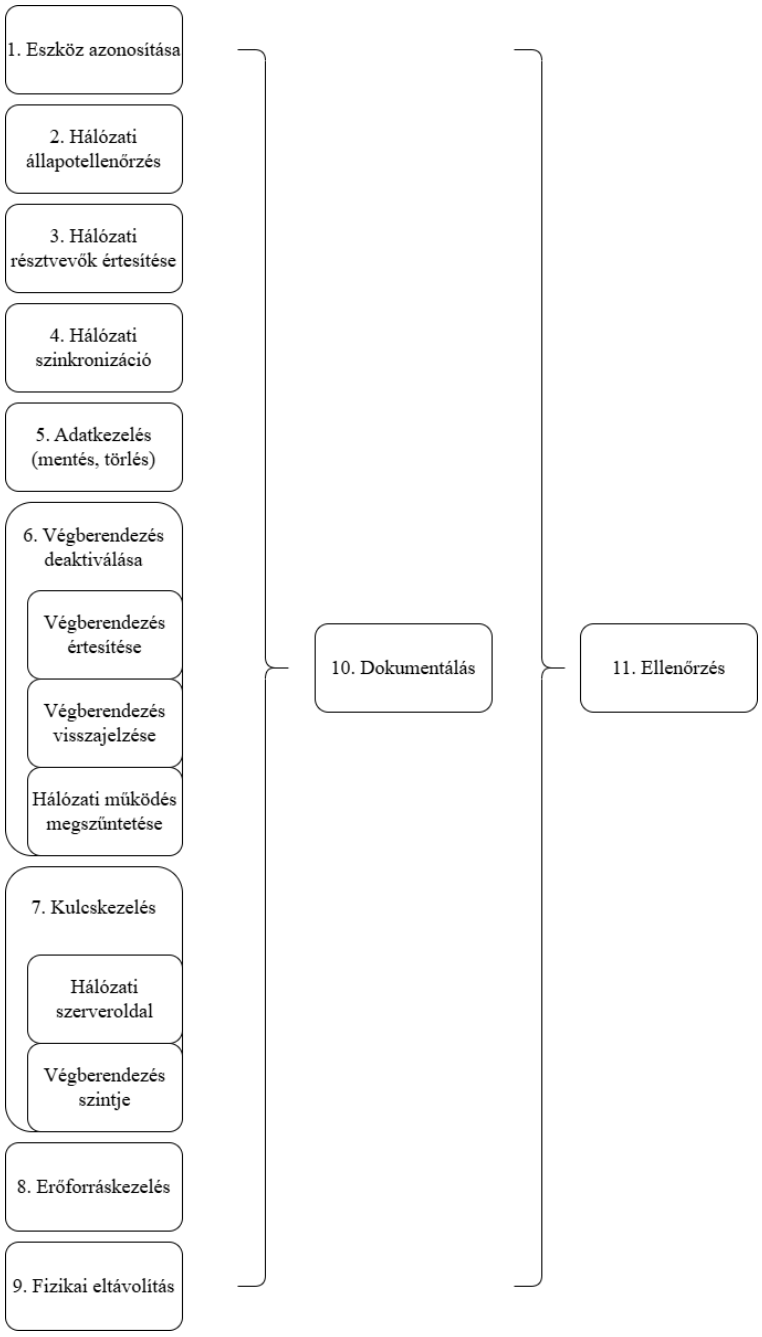
A harmadik lépés az *állapotkonzisztencia biztosítása*, miszerint az érintett rétegek kezelése is megtörténik. Itt kell a kapcsolódó nyilvántartásokat frissíteni, felszabadítani a nem használt erőforrásokat, szükség esetén az archiválást és törlést végrehajtani, az érintett rendszerkomponenseket szinkronizálni. Kivonás csak akkor tekinthető sikeresnek, ha az adott eszköz minden architekturális rétegben inaktív/kivont állapotba került.

A negyedik, lezáró lépés, a *verifikáció és audit*, amely a kivonási folyamat eredményét ellenőrzi és dokumentálja. Ez magában foglalja az eszköz és az érintett rétegek végállapotának ellenőrzését, a lépések naplózását, a felmerülő problémák rögzítését és a fizikai eltávolítást. Ez a lépés biztosítja azt, hogy a végrehajtott kivonási műveletsorozat lezárható és ellenőrizhető legyen.

A modell nem technológiafüggő, így alkalmazható különböző IoT-alapú személy- és vagyonvédelemben alkalmazott végberendezések esetében is. A következő fejezet foglalkozik a modell konkrét leképezésével LoRaWAN végberendezések esetére.

5.5 Javasolt kivonási eljárás módszer LoRaWAN-alapú IoT személy- és vagyonvédelem területén alkalmazott végpontokra

A LoRaWAN kommunikáció jellemzői és a specifikációk értelmezése, hiányossága már korábbi fejezetekben ismertetésre került, így ezen fejezet a továbbiakban a már összefoglalt információkra épít és csak a szükséges mértékben ismétli azokat. Azt viszont fontosnak tartom ismételten kiemelni, hogy a LoRaWAN specifikációk és a kapcsolódó dokumentációk a végberendezések kivonási eljárását csupán említés szintjén jelenítik meg, de nem adnak meg egy dedikált módszert, lépéssorozatot. Utalás viszont található arra, hogy ezt javasolt alkalmazás szintjén megvalósítani [48][57], ami a LoRaWAN végpontok kivonási eljárását az implementációs és üzemeltetési rétegbe helyezi. A feldolgozott szakirodalomban megjelenik, mint specifikációs hiányosság [58][128], de azok sem kínálnak kidolgozott módszertant rá [129][7]. A LoRaWAN végpontok kivonási eljárásának kidolgozása során az általános IoT architektúrákat, kapcsolódó szabványokat és ajánlásokat, valamint a LoRaWAN specifikus dokumentumokat használtam alapul, építve az elvégzett mérési eredményeimre. A folyamatot a 16. ábra foglalja össze. [72]



16. ábra - LoRaWAN végpont kivonási folyamata (Készítette a szerző: [72])

A LoRaWAN végpontok kivonási eljárásának első lépése az *eszköz azonosítása*, amely DevEUI alapján történik. Ez az azonosító egyedi a hálózaton belül, így egyértelmű azonosítást tesz lehetővé, amely elengedhetetlen a folyamat megkezdéséhez. A második lépés a *hálózati állapotellenőrzés*, ahol vizsgálni kell a végpont aktuális hálózati aktivitását és kommunikációs státuszát, hogy ténylegesen indokolt-e a folyamat végrehajtása. A harmadik lépés a *hálózati résztvevők értesítése* a kivonási eljárásról. A lépés során minden olyan hálózati elemet értesíteni kell a kivonási eljárásról, amelyek azonosítók és kulcsok tárolásáért felelősek, hálózatmenedzsment adatokat kezelnek,

üzenettovábbításban részt vesznek, titkosítást és dekódolást, visszafejtést végeznek, adatmentésért felelősek. E ponton válik egyértelművé a folyamat többrétegű jellege. A negyedik lépés a *hálózati szinkronizáció*, amely a 3-as lépésnél érintett hálózati résztvevők felkészülését jelenti a műveletre. Az ötös lépés az *adatok mentése és törlése*. Amennyiben a végberendezés által szolgáltatott adatok adminisztrációs céllal a későbbiekben szükségesek, így azok mentése javasolt, ellenkező esetben törlésük. Látható, hogy az 1-5. lépések előkészítő jellegűek, tényleges beavatkozás még nem történik.

A hatos lépés, a *végberendezés deaktiválása*, a végberendezés érintettségéből a legjelentősebb lépés, három alfolyamatot foglal magában. Először a végberendezést értesíteni kell a hálózati kommunikáció megszüntetéséről valamilyen dedikált formában. A kommunikáció sajátossága miatt, illetve meghibásodás következtében, ennek megérkezése nem garantált, így hibakezelés beiktatása szükséges lehet. Ha a végberendezés fogadta ezt az értesítést és visszajelzést küldött, nyugtázta a kérést, akkor meg kell szüntetnie a további hálózati kommunikációját. Ha nem érkezik visszajelzés ismételt próbálkozást követően sem (érdemes limitálni a próbálkozások számát), akkor helyszíni, manuális beavatkozás szükséges.

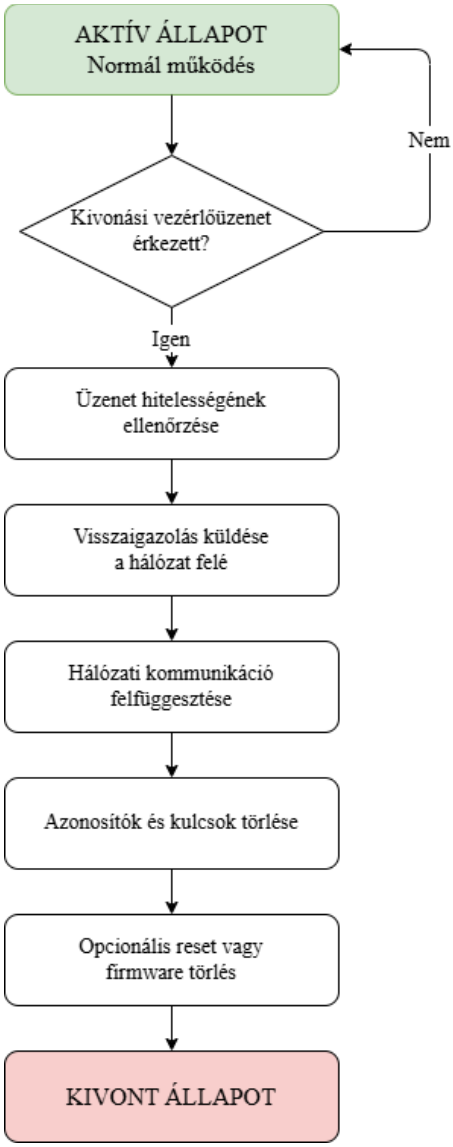
A hetes lépés a *kulcskezelés*, amikor a kulcsok, azonosítók eltávolítása történik eszközoldalon és hálózati szerveroldalon egyaránt. Ez akadályozza meg azt, hogy az eszköz további hálózati műveleteket hajthasson végre, illetve az újbóli felhasználhatóságot. A nyolcas lépés az *erőforrások felszabadítása*, ahol a végberendezéshez kapcsolódó adatok eltávolítása történik minden listából és helyről.

A kilences lépés, a *fizikai eltávolítás*, sorrendben nem feltétlenül a kilencedik, mivel a végberendezés állapotától függően a 6-os, 7-es vagy 8-as lépés elé kerül vagy azokkal akár párhuzamosan is végezhető. Illetve, a fizikai eltávolítás csak akkor része a folyamatnak, ha az adott eszköz véglegesen kikerül a rendszerből és ott nem használják fel újból.

A *dokumentálás* és *ellenőrzés* lépéseknek a teljes folyamat során meg kell jelennie. A folyamat egészét, minden műveletét dokumentálni kell, ahol rögzítésre kerül a végrehajtott feladat, az érintett elemek, hibák és rendellenességek. Minden eszköz kivonási eljárása után és közben ellenőrizni kell, hogy a hálózat továbbra is megfelelően működik-e, és hogy az alkalmazás a várt funkciókat ellátja. Ezenkívül felülvizsgálni kell,

hogy a végberendezés leállította-e hálózati tevékenységét. Ha az eszköz továbbra is aktív a hálózaton, a lépéseket meg kell ismételni, és szükség esetén a beépített mechanizmus és a folyamat módosítása szükségessé válhat.

A 17. ábra szemlélteti kizárólag a végberendezés-oldali folyamatokat normál működés mellett.



17. ábra - A kivonási eljárás végberendezés-oldali folyamata normál működés mellett

A végberendezés a normál, aktív állapotból egy dedikált vezérlőüzenet (nem specifikáció meghatározott, javaslat) hatására a már korábban részletezett, előre meghatározott lépéssorozaton halad végig, amely biztosítja a kommunikáció megszűntetését és a kriptográfiai kontextus lezárását.

Amennyiben az eszköz fizikai vagy szoftveres hibája miatt nem képes hálózati kommunikációra, a dedikált értesítési lépés és az eszközoldali kulcstörlés nem hajtható végre automatizáltan, ahogy az a vonatkozó lépésnél is említésre került. Ilyen esetben a hálózati oldali kulcsvisszavonás, az erőforrás-felszabadítás és a fizikai eltávolítás végrehajtása szükséges. Ha a végberendezés javításra szorul, akkor javasolt a kivonási eljárás teljes végrehajtását előfeltételnek tekinteni az újbóli üzembe helyezéshez.

Az ismertetett kivonási eljárás rámutat arra, hogy a LoRaWAN-alapú IoT végpontok esetében sem redukálható egyetlen adminisztratív műveletre vagy fizikai eltávolításra a kivonási eljárás. Bár a LoRaWAN specifikációk részletesen szabályozzák az aktiválási és hitelesítési folyamatokat, ugyanakkor a kivonás protokollszintű, dedikált mechanizmusként nem jelenik meg. Az ismertetett lépéssor egy olyan determinisztikus, dokumentálható és többkomponensű folyamatot ír le, amely biztosítja a végpont fizikai, logikai állapotának következetes, és ellenőrizhető lezárását.

5.6 A kivonási eljárás szerepe az integrált védelmi megbízhatósági keretrendszerben

A korábbi fejezetekben ismertetett és validált integrált megbízhatósági keretrendszer eredménye, hogy az IoT-alapú személy- és vagyonvédelmi végberendezések, rendszerek megbízhatósága nem csupán kommunikációs paraméterek függvénye, hanem kontextuális, funkcionális, strukturális és életciklus-alapú tényezők összességének eredménye. Az eszköz-életciklus megfelelő lezárása a modell alapján nem adminisztratív elemként értelmezhető, hanem megbízhatósági állapotényezőként. Ha egy IoT végpont fizikailag eltávolításra kerül, funkcionálisan működése inaktív vagy nem releváns, incidens miatt működése problémát, rendszerszintű hatást okoz, de logikai állapota továbbra is fennmarad, akkor ez a rendszerszintű értékelésben inkonzisztenciát okoz. Ez azt jelenti, hogy a végberendezések továbbra is részei a nyilvántartásoknak, de nem részei az operatív struktúrának.

A megbízhatósági keretrendszerben a kivonási eljárás több dimenzióra is hatással van. A végberendezések száma, azok kapcsolatai és jogosultsági kérdései csak akkor mutatják a valós állapotot, ha a kivont végberendezés minden rétegben (S) lekezelésre került. A funkcionális (F) működés valós értékelése csak akkor lehetséges, ha minden végpont ténylegesen működőképes és hiteles. A hibásan működő vagy „szellem eszközök” jelenléte torzítja az értékelést és időbeli (T) problémák kialakulását eredményezheti. Az

életciklus-menedzsment (L) során a végberendezés életciklusának lezárása egy kritikus pont, melynek nem megfelelő kontrollálása hosszútávú és rendszerszintű hatásként jelentkezik.

Összefoglalva, a kivonási eljárás relevanciáját:

- csökkenti a rejtett kockázatokat,
- gátolja a jogosulatlan újra-aktiválási lehetőséget,
- biztosítja a logikai és kriptográfiai kontextus lezárást,
- segíti az auditálhatóságot,
- hozzájárul a rendszer állapottranszparenciájához.

Megalkotott modell alapján kijelenthető, hogy a kivonási eljárás az IoT-alapú (és ezen belül a LoRaWAN-alapú) személy- és vagyonvédelmi rendszerekben nem elhanyagolható, hiszen a megbízhatósági keretrendszer meghatározó, elengedhetetlen eleme.

5.7 Összegzés, következtetések

A fejezet egyik fő célja volt annak igazolása, hogy az IoT-alapú személy- és vagyonvédelmi rendszerekben az eszköz-életciklus megfelelő kezelése - különös tekintettel a kivonási eljárásra – biztonságtechnikai szempontból kiemelt és meghatározó jelentőségű. A fejezet másik fő célja az volt, hogy egy olyan módszer, eljárásrend kerüljön kidolgozásra, mely ezt ellenőrizhető, reprodukálható, strukturált módon megvalósítja.

Az elemzéseim és vizsgálataim rámutattak arra, hogy az IoT-eszközök életciklusa nem tekinthető lezártnak a fizikai eszköz eltávolításával. A LoRaWAN specifikációk és kiegészítő dokumentációk nem tartalmaznak dedikált kivonási mechanizmust, a tudományos publikációk is hiányosságként emelik azt ki. Ha a kivonás nem strukturáltan történik, akkor az rejtett kockázatok kialakulásához és a megbízhatóság torzulásához vezethet. A kulcs- és jogosultságkezelés nem hagyható figyelmen kívül a kivonási eljárás során. A javasolt IoT-életciklus-lezárási modell és annak LoRaWAN-specifikus kifejtése egy strukturált, többfázisú megközelítést biztosít.

Igazoltam, hogy az IoT-végpontok kivonása az életciklus-menedzsment kiemelten fontos eleme, a rendszer biztonsági állapotát strukturálisan módosító folyamat. Feltártam a fizikai-logikai szétválásból eredő jelenséget, mint a kivonás alapvető problémáját.

Kidolgoztam egy determinisztikus, auditálható és többrétegű IoT-életciklus-lezárási modellt és annak LoRaWAN végpontokra megfeleltetett kivonási eljárását, amely biztosítja a fizikai, logikai és biztonsági/hitelesítési kontextus, a rendszerállapot és az erőforrások ellenőrizhető lezárását, valamint csökkenti a rejtett kockázatokat. A fejezet megalapozza és igazolja a negyedik hipotézis (H4) helytállóságát. A kapcsolódó kutatási eredmények lektorált tudományos közleményben [72] jelentek meg, amelyre nemzetközi hivatkozás is értekezett.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Értekezésem és kutatásaim középpontjában az IoT-alapú megoldások, különösen a LoRaWAN, személy- és vagyonvédelmi rendszerekben történő alkalmazhatósága állt. A téma aktualitását mutatja az IoT-technológiák rohamos fejlődése és elterjedése, valamint az IoT érzékelőhálózatokra és vezetéknélküli kommunikációs megoldásokra épülő védelmi rendszerek növekvő alkalmazása. Az IoT-alapú rendszerek számos előnyt biztosítanak például kiterjedt objektumok monitorozására, távoli felügyeleti megoldásokban és az automatizált működés biztosításában, de működési sajátosságaik és korlátaik új kutatási kérdéseket vetnek fel biztonságtechnikai aspektusban.

A tématerülethez kapcsolódó nemzetközi és hazai szakirodalom feldolgozásával indítottam kutatásaimat, mely végig jelen volt a teljes folyamatban, különös tekintette az IoT és LPWAN működési sajátosságaira és fellelhető alkalmazási korlátaira. Második lépésben empirikus, nagymintás vizsgálatokat végeztem két időpontban a tanúsított LoRaWAN végberendezések körében. Az elemzés eredményeként azonosítottam azokat a mintázatokat, amelyek a technológia alkalmazhatóságát befolyásolják, valamint kialakítottam a LoRaWAN végpontok funkcionális csoportosítását. Kutatásom során megalkottam az IoT-alapú védelmi rendszer fogalmi keretét és kidolgoztam az IoT végpontok biztonságtechnikai megbízhatóságát többdimenziós modell formájában. A megbízhatósági modell és az abból levezetett kockázati osztályozás felhasználható a végpontok alkalmazhatóságának értékelésére és összehasonlítására. A modell gyakorlati érvényességét és a dimenziók közötti hatásokat mérésekkel és kísérletekkel igazoltam. A kutatásom utolsó részének fontos eredménye az IoT-végpontok életciklus-menedzsmentjének vizsgálatából kidolgozott általános IoT-életciklus-lezárási modell, valamint a LoRaWAN végpontokra adaptált kivonási eljárás volt.

Az értekezés a kutatómunkám eredményeit logikai ívbe rendezve mutatja be: először az elméleti és technológiai megalapozást ismerteti (1. fejezet), amelyet a tanúsított LoRaWAN végpontok empirikus vizsgálata követ (2. fejezet). Ezután következik a kutatás során kialakított fogalmi és modellalkotási keret bemutatása (3. fejezet), majd a modell gyakorlati validációja mérési és kísérleti eredmények alapján valósul meg (4. fejezet). Az értekezés záró fejezete az IoT-végpontok életciklus-lezárásának kérdéseit tárgyalja, valamint ismerteti a kidolgozott kivonási modellt (5. fejezet).

Új tudományos eredmények

Értekezésem elkészítése során négy összetett hipotézist (H1-H4) vizsgáltam, melyekkel kapcsolatosan az alábbi megállapításokat teszem. Az értekezés tézisei (T1-T4):

T1: Két eltérő időpontban végzett, nagymintás empirikus vizsgálat alapján elvégeztem a tanúsított LoRaWAN végberendezések strukturált elemzését és kialakítottam azok funkcionális tipológiáját. Igazoltam, hogy a tanúsított eszközállomány visszatérő mintázatokat mutat – különösen a detektálási/jelzési funkcionális dominancia, az eseményvezérelt kommunikáció korlátozó jellege, a specifikációs és működési heterogenitás, valamint a termékportfólió fluktuációjából adódó életciklus-instabilitás tekintetében –, amelyek rendszerszinten meghatározzák a személy- és vagyonvédelmi alkalmazhatóság korlátait.

T2: Megalkottam az IoT-alapú elektronikai védelmi rendszer fogalmát, valamint többrétegű értelmezési modelljét, továbbá kidolgoztam az IoT-végpontok biztonságtechnikai megbízhatóságának 4+1 dimenziós (F, T, C, L, S) modelljét, amely a megbízhatóságot a védelmi cél teljesítésére való alkalmasságként értelmezi és azt 0-1 tartományú indexként határoztam meg. A modell alapján kialakítottam a funkcionális végpont-kockázati osztályokat (K1-K4), amelyek lehetővé teszik a heterogén IoT-végpontok összehasonlítását személy- és vagyonvédelmi környezetben.

T3: Mérésekkel és kísérletekkel igazoltam, hogy a többdimenziós megbízhatósági modell dimenziói mérhető hatást gyakorolnak a LoRaWAN-alapú IoT-végpontok személy- és vagyonvédelmi szempontból releváns működésére, valamint hogy azonosíthatók a dimenziók közötti kölcsönhatások. Kimutattam, hogy a kontextuális és életciklus-tényezők nemlineáris módon befolyásolják a végpontok működési stabilitását, továbbá azt, hogy a funkcionális dimenzió paraméterezésének optimalizálása bizonyos mértékű kompenzációt tesz lehetővé, ugyanakkor kompromisszumokkal jár.

T4: Igazoltam, hogy az IoT-végpontok megfelelő életciklus-lezárásának hiányában a fizikai és logikai állapot inkonzisztenciája állhat fenn, amely befolyásolja az IoT-alapú személy- és vagyonvédelmi rendszerek megbízhatóságát, rejtett kockázatokat eredményez és torzítja a rendszerállapot értékelését. Ennek kezelésére kidolgoztam egy általános IoT-életciklus lezárási modellt, valamint ezt adaptáltam LoRaWAN IoT-végpontok kivonására is.

Ajánlások, eredmények hasznosíthatósága

Az értekezésben ismertetett kutatási eredményeket gyakorlati szempontból elsősorban az IoT-alapú személy- és vagyonvédelmi rendszerek tervezésében, értékelésében és üzemeltetésében lehet hasznosítani. A vizsgált eszközök, a kidolgozott fogalmi keretek, modellek, osztályozások és eljárások lehetőséget biztosítanak arra, hogy az IoT-végpontok alkalmazhatósága ne kizárólag kommunikációs vagy technológiai paraméterek alapján kerüljön megítélésre, hanem figyelembe vegye a működési körülményeket, a funkcionális sajátosságokat, valamint az eszközök életciklus-állapotát is. Ez a fajta új megközelítés hozzájárulhat a tervezési döntések megalapozásához, valamint a különböző IoT-megoldások biztonságtechnikai szempontú értékeléséhez és összehasonlításához.

A kutatási eredményeim ezek mellett módszertani támogatást biztosítanak a személy- és vagyonvédelmi rendszerek fejlesztésével és üzemeltetésével foglalkozó szakemberek részére is. Az ismertetett modell és a hozzá kapcsolódó kockázati osztályok alkalmazhatók lehetnek IoT-alapú rendszerek értékelése, auditálása, kockázatelemzése, tervezési folyamatai és üzemeltetése során. Az IoT-végpontok életciklus-lezárására vonatkozó megállapítások és a LoRaWAN végpontokra kidolgozott kivonási eljárás pedig hozzájárulhat az ilyen rendszerek hosszú távú megbízhatóságának fenntartásához, valamint a rejtett kockázatok csökkentéséhez, kezeléséhez.

Az értekezés eredményei az alábbi területek szakmai szereplői számára hasznosíthatók a leginkább:

- Biztonságtechnikai rendszerek tervezői és integrátorai számára a megfelelő megoldások kiválasztásához.
- Biztonságtechnikai szolgáltatók és üzemeltetők részére rendszerértékelés és a kockázatok azonosítására.
- IoT-eszközök és rendszerek fejlesztőinek a megfelelő módszerek implementálásához.
- Auditorok és kockázatelemzéssel foglalkozó szakemberek számára a strukturált rendszerértékeléshez.
- Kritikus infrastruktúrák, ipari IoT és Ipar 4.0 területén dolgozó mérnök és kiberbiztonsági szakemberek számára a rendszerek és megoldások értékeléséhez.
- Szakmai és szabályozási szerveknek irányelvek és ajánlások kidolgozásához.

- Kutatók, oktatók részére további elemzésekhez és tudományos vizsgálatokhoz.

A kutatási eredmények hozzájárulhatnak az IoT-alapú személy- és vagyonvédelmi rendszerek tudatosabb tervezéséhez, értékeléséhez és üzemeltetéséhez, valamint alapot nyújthatnak a technológia alkalmazásainak további fejlesztéséhez.

Új kutatási irányok, lehetőségek

Az értekezés eredményei alapján több új kutatási irányt is ki lehet emelni. Az értekezés logikai évéhez szorosan kapcsolódva, a modellek és vizsgálatok kiterjeszthetők más hálózati architektúrájú rendszereke. Ezek az új irányok [130] további mélységet eredményeznek és hozzájárulnak az értelmezések további finomításához.

Az alkalmazási terület kiterjesztésének egyik ilyen lehetősége az IoT-alapú kommunikációs rendszerek alkalmazásának és szerepének vizsgálata komplex rendszerekben, kifejezetten okos városok (Smart City) infrastruktúráiban az alrendszerek közötti adattovábbítás tekintetében. A másik lehetséges irány a kritikus infrastruktúrák védelmét támogató és megvalósító IoT megoldások elemzése.

Eltérő, bár nagyon aktuális terület a mesterséges intelligencia és a gépi tanulási módszerek integrálása a rendszerek működésének vizsgálatához. A nagymennyiségű kommunikációra és működésre vonatkozó adatok felhasználhatók olyan modellek kialakítására, mely alkalmas prediktív becslésre, anomáliák korai felismerésére, valamint valós idejű állapotértékelésre.

IRODALOMJEGYZÉK

[1] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, és S. Clarke, „Middleware for Internet of Things: A Survey”, *IEEE Internet Things J.*, köt. 3, sz. 1, o. 70–95, febr. 2016, doi: 10.1109/JIOT.2015.2498900.

[2] N. Srivastava és P. Pandey, „Internet of things (IoT): Applications, trends, issues and challenges”, *Mater. Today Proc.*, köt. 69, o. 587–591, 2022, doi: 10.1016/j.matpr.2022.09.490.

[3] H. Park és S. Park, „Emerging Trends and Challenges in IoT Networks”, *Electronics (Basel).*, köt. 13, sz. 3, o. 513, jan. 2024, doi: 10.3390/electronics13030513.

[4] K. M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou, és C. de Vaulx, „Trends and Challenges in AIoT/IIoT/IoT Implementation”, *Sensors*, köt. 23, sz. 11, o. 5074, máj. 2023, doi: 10.3390/s23115074.

[5] L. L. Knud, „IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year”, IoT Analytics. Elérés: 2024. február 4. [Online]. Elérhető: https://iot-analytics.com/iot-2019-in-review/

[6] I. Cvitić, D. Peraković, M. Periša, A. Jevremović, és A. Shalaginov, „An Overview of Smart Home IoT Trends and related Cybersecurity Challenges”, *Mobile Networks and Applications*, köt. 28, sz. 4, o. 1334–1348, aug. 2023, doi: 10.1007/s11036-022-02055-w.

[7] M. Centenaro, L. Vangelista, A. Zanella, és M. Zorzi, „Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios”, *IEEE Wirel. Commun.*, köt. 23, sz. 5, o. 60–67, okt. 2016, doi: 10.1109/MWC.2016.7721743.

[8] N. S. Sayem *és mtsai.*, „IoT-based smart protection system to address agro-farm security challenges in Bangladesh”, *Smart Agricultural Technology*, köt. 6, o. 100358, dec. 2023, doi: 10.1016/j.atech.2023.100358.

[9] D. Borsos, „A LoRaWAN-technológia szerepe az elektronikai védelem területén, az építőipari beruházások vonatkozásában”, *Hadmérnök*, köt. 16, sz. 3, o. 5–16, nov. 2021, doi: 10.32567/hm.2021.3.1.

[10] F. Bálint és R. Pető, „Sustainable and Safe Cities through Computer Applications”, *Interdisciplinary Description of Complex Systems*, köt. 23, sz. 3, o. 207–216, 2025, doi: 10.7906/indecs.23.3.2.

[11] A. Karkouch, H. Mousannif, H. Al Moatassime, és T. Noel, „Data quality in internet of things: A state-of-the-art survey”, *Journal of Network and Computer Applications*, köt. 73, o. 57–81, szept. 2016, doi: 10.1016/j.jnca.2016.08.002.

[12] L. Berek, L. Berek, és Z. Rajnai, *A tudományos kutatás folyamata és módszerei*. Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2018. Elérés: 2025. december 6. [Online]. Elérhető: https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/25308/Berek_Berek_Rajnai_Tudkut_2022.pdf?sequence=1&isAllowed=y

[13] L. L. Knud, „Top 10 IoT applications in 2020”, IoT Analytics. Elérés: 2024. május 4. [Online]. Elérhető: https://iot-analytics.com/top-10-iot-applications-in-2020/

[14] M. Asemani, F. Abdollahei, és F. Jabbari, „Understanding IoT Platforms : Towards a comprehensive definition and main characteristic description”, in *2019 5th International Conference on Web Research (ICWR)*, IEEE, ápr. 2019, o. 172–177. doi: 10.1109/ICWR.2019.8765259.

[15] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, és P. Urien, „Internet of Things: A Definition & Taxonomy”, in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, IEEE, szept. 2015, o. 72–77. doi: 10.1109/NGMAST.2015.71.

[16] L. Atzori, A. Iera, és G. Morabito, „Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm”, *Ad Hoc Networks*, köt. 56, o. 122–140, márc. 2017, doi: 10.1016/j.adhoc.2016.12.004.

[17] K. Sorri, N. Mustafee, és M. Seppänen, „Revisiting IoT definitions: A framework towards comprehensive use”, *Technol. Forecast. Soc. Change*, köt. 179, o. 121623, jún. 2022, doi: 10.1016/j.techfore.2022.121623.

[18] R. Minerva, A. Biru, és D. Rotondi, „Towards a definition of the Internet of Things (IoT)”, máj. 2014. Elérés: 2025. március 4. [Online]. Elérhető:

https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[19] L. Da Xu, W. He, és S. Li, „Internet of Things in Industries: A Survey”, *IEEE Trans. Industr. Inform.*, köt. 10, sz. 4, o. 2233–2243, nov. 2014, doi: 10.1109/TII.2014.2300753.

[20] D. Borsos, „Bevezetés a személy- és vagyonvédelem területén alkalmazható IoT technológiákba – LoRaWAN technológia”, in *XXXV. Jubileumi Kandó Konferencia 2019*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 94–102.

[21] L. L. Knud, „State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time”, IoT Analytics. Elérés: 2024. március 1. [Online]. Elérhető: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

[22] P. J. Basford, F. M. J. Bulot, M. Apetroaie-Cristea, S. J. Cox, és S. J. Ossont, „LoRaWAN for Smart City IoT Deployments: A Long Term Evaluation”, *Sensors*, köt. 20, sz. 3, o. 648, jan. 2020, doi: 10.3390/s20030648.

[23] S. Satyajit, „State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally”, IoT Analytics. Elérés: 2025. december 4. [Online]. Elérhető: https://iot-analytics.com/number-connected-iot-devices/

[24] „Internet Of Things Market Size & Share Analysis - Growth Trends And Forecast (2025 - 2030)”, Mordor Intelligence. Elérés: 2025. november 5. [Online]. Elérhető: https://www.mordorintelligence.com/industry-reports/internet-of-things-iot-market

[25] ISO/IEC 21823:2019, *Internet of things (IoT) — Interoperability for IoT systems*. ISO, 2019.

[26] ISO/IEC 27400:2022, *Cybersecurity — IoT security and privacy — Guidelines*. ISO, 2022.

[27] ETSI EN 303 645, *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*. ETSI, 2024. Elérés: 2024. július 6. [Online]. Elérhető:

https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/03.01.01_60/ts_103645v030101p.pdf

[28] ISO/IEC 30141:2024, *Internet of Things (IoT) — Reference architecture*. ISO, 2024.

[29] G. Breda, P. J. Varga, és Z. Illesi, „Forensic Functional Profile of loT Devices-Based on Common Criteria”, in *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, szept. 2018, o. 000261–000264. doi: 10.1109/SISY.2018.8524813.

[30] J. A. López-Pastor, M. Poveda-García, A. Gil-Martínez, D. Cañete-Rebenaque, és J. L. Gómez-Tornero, „2-D Localization System for Mobile IoT Devices Using a Single Wi-Fi Access Point With a Passive Frequency-Scanned Antenna”, *IEEE Internet Things J.*, köt. 10, sz. 17, o. 14995–15011, szept. 2023, doi: 10.1109/JIOT.2023.3262830.

[31] G. Koulouras, S. Katsoulis, és F. Zantalis, „Evolution of Bluetooth Technology: BLE in the IoT Ecosystem”, *Sensors*, köt. 25, sz. 4, o. 996, febr. 2025, doi: 10.3390/s25040996.

[32] A. Zohourian *és mtsai.*, „IoT Zigbee device security: A comprehensive review”, *Internet of Things*, köt. 22, o. 100791, júl. 2023, doi: 10.1016/j.iot.2023.100791.

[33] G. Qiu, W. Tao, R.-C. Hwang, és C. Xie, „Wide-Area Visual Monitoring System Based on NB-IoT”, *Sensors*, köt. 25, sz. 21, o. 6589, okt. 2025, doi: 10.3390/s25216589.

[34] N. H. Qasim, A. J. Salman, H. M. Salman, A. A. AbdelRahman, és A. Kondakova, „Evaluating NB-IoT within LTE Networks for Enhanced IoT Connectivity”, in *2024 35th Conference of Open Innovations Association (FRUCT)*, IEEE, ápr. 2024, o. 552–559. doi: 10.23919/FRUCT61870.2024.10516400.

[35] H. A. K. M. Bahalul, M. Z. Md. Oahiduzzaman, és H. Md. Rifat, „5G and Internet of Things—Integration Trends, Opportunities, and Future Research Avenues”, in *5G and Beyond*, Springer, Singapore: Springer Tracts in Electrical and Electronics Engineering, 2023, o. 217–245. doi: 10.1007/978-981-99-3668-7_11.

[36] A. Ilyin, A. Matinyan, A. Rolich, és L. Voskov, „Experimental Evaluation of Iridium Performance under Varying Weather Conditions and Elevation Angles”, in *2024 International Seminar on Electron Devices Design and Production (SED)*, IEEE, okt. 2024, o. 1–5. doi: 10.1109/SED63331.2024.10741060.

[37] A. Andreadis, G. Giambene, és R. Zambon, „Latency Analysis for Satellite IoT in Remote Areas”, in *2025 IEEE 21st International Conference on Factory Communication Systems (WFCS)*, IEEE, jún. 2025, o. 1–8. doi: 10.1109/WFCS63373.2025.11077635.

[38] G. Boquet, B. Martinez, F. Adelantado, J. Pages, J. A. Ruiz-de-Azua, és X. Vilajosana, „Low-Power Satellite Access Time Estimation for Internet of Things Services Over Nonterrestrial Networks”, *IEEE Internet Things J.*, köt. 11, sz. 2, o. 3206–3216, jan. 2024, doi: 10.1109/JIOT.2023.3298017.

[39] A. Feijoo-Añazco, D. Garcia-Carrillo, J. Sanchez-Gomez, és R. Marin-Perez, „Innovative security and compression for constrained IoT networks”, *Internet of Things*, köt. 24, o. 100899, dec. 2023, doi: 10.1016/j.iot.2023.100899.

[40] D. Orlovs, A. Rusins, V. Skrastiņš, és J. Judvaitis, „LPWAN Technologies for IoT: Real-World Deployment Performance and Practical Comparison”, *IoT*, köt. 6, sz. 4, o. 77, dec. 2025, doi: 10.3390/iot6040077.

[41] P. Ruckebusch, S. Giannoulis, I. Moerman, J. Hoebeke, és E. De Poorter, „Modelling the energy consumption for over-the-air software updates in LPWAN networks: SigFox, LoRa and IEEE 802.15.4g”, *Internet of Things*, köt. 3–4, o. 104–119, okt. 2018, doi: 10.1016/j.iot.2018.09.010.

[42] S. Satyajit, „Global LPWAN Market Tracker and Forecast 2015-2027 (Q1/2024 Update)”, IoT Analytics. Elérés: 2025. május 5. [Online]. Elérhető: https://iot-analytics.com/product/global-lpwan-market-tracker-and-forecast-2015-2027-q1-2024-update/

[43] R. S. Sinha, Y. Wei, és S.-H. Hwang, „A survey on LPWA technology: LoRa and NB-IoT”, *ICT Express*, köt. 3, sz. 1, o. 14–21, márc. 2017, doi: 10.1016/j.icte.2017.03.004.

[44] A. Lavric, A. I. Petrariu, és V. Popa, „Long Range SigFox Communication Protocol Scalability Analysis Under Large-Scale, High-Density Conditions”, *IEEE Access*, köt. 7, o. 35816–35825, 2019, doi: 10.1109/ACCESS.2019.2903157.

[45] A. M. Abbas, K. Y. Youssef, I. I. Mahmoud, és A. Zekry, „NB-IoT optimization for smart meters networks of smart cities: Case study”, *Alexandria Engineering Journal*, köt. 59, sz. 6, o. 4267–4281, dec. 2020, doi: 10.1016/j.aej.2020.07.030.

[46] B. Miles, E.-B. Bourennane, S. Boucherkha, és S. Chikhi, „A study of LoRaWAN protocol performance for IoT applications in smart agriculture”, *Comput. Commun.*, köt. 164, o. 148–157, dec. 2020, doi: 10.1016/j.comcom.2020.10.009.

[47] K. Mekki, E. Bajic, F. Chaxel, és F. Meyer, „A comparative study of LPWAN technologies for large-scale IoT deployment”, *ICT Express*, köt. 5, sz. 1, o. 1–7, márc. 2019, doi: 10.1016/j.icte.2017.12.005.

[48] LoRa Alliance, *LoRaWAN® Specification v1.0*. 2015. Elérés: 2023. február 5. [Online]. Elérhető: https://lora-alliance.org/sites/default/files/2018-05/2015_-_lorawan_specification_1r0_611_1.pdf

[49] H. Mroue *és mtsai.*, „LoRa+: An extension of LoRaWAN protocol to reduce infrastructure costs by improving the Quality of Service”, *Internet of Things*, köt. 9, o. 100176, márc. 2020, doi: 10.1016/j.iot.2020.100176.

[50] A. D. Zayas és P. Merino, „The 3GPP NB-IoT system architecture for the Internet of Things”, in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE, máj. 2017, o. 277–282. doi: 10.1109/ICCW.2017.7962670.

[51] LoRa Alliance, „About LoRa Alliance®”. Elérés: 2020. január 12. [Online]. Elérhető: https://lora-alliance.org/about-lora-alliance/

[52] D. Hunt, „LoRa Alliance Certification”, *Journal of ICT Standardization*, köt. 9, sz. 1, o. 13–20, ápr. 2021, doi: 10.13052/jicts2245-800X.912.

[53] LoRa Alliance, *LoRaWAN® Specification v1.0.1*. 2016. Elérés: 2025. december 5. [Online]. Elérhető: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-0-1

[54] LoRa Alliance, *LoRaWAN® Specification v1.0.2*. 2016. Elérés: 2026. január 15. [Online]. Elérhető: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-0-2

[55] LoRa Alliance, *LoRaWAN® Specification v1.0.3*. 2018. Elérés: 2025. április 5. [Online]. Elérhető: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-0-3

[56] LoRa Alliance, *TS001-1.0.4 LoRaWAN® L2 1.0.4 Specification*. 2020. Elérés: 2026. január 4. [Online]. Elérhető: https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification

[57] LoRa Alliance, *LoRaWAN® Specification v1.1*. 2017. Elérés: 2024. augusztus 4. [Online]. Elérhető: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1

[58] I. Butun, N. Pereira, és M. Gidlund, „Security Risk Analysis of LoRaWAN and Future Directions”, *Future Internet*, köt. 11, sz. 1, o. 3, dec. 2018, doi: 10.3390/fi11010003.

[59] S. Loukil, L. C. Fourati, A. Nayyar, és C. So-In, „Investigation on Security Risk of LoRaWAN: Compatibility Scenarios”, *IEEE Access*, köt. 10, o. 101825–101843, 2022, doi: 10.1109/ACCESS.2022.3208171.

[60] LoRa Alliance, *TS002-1.1.0 LoRaWAN® Backend Interfaces*. 2020. Elérés: 2024. május 11. [Online]. Elérhető: https://resources.lora-alliance.org/technical-specifications/ts002-1-1-0-lorawan-backend-interfaces

[61] M. Alipio és M. Bures, „Current testing and performance evaluation methodologies of LoRa and LoRaWAN in IoT applications: Classification, issues, and future directives”, *Internet of Things*, köt. 25, o. 101053, ápr. 2024, doi: 10.1016/j.iot.2023.101053.

[62] R. Carvalho, N. Correia, és F. Al-Tam, „Mobility planning of LoRa gateways for edge storage of IoT data”, *Computer Networks*, köt. 221, o. 109521, febr. 2023, doi: 10.1016/j.comnet.2022.109521.

[63] J. R. Cotrim és J. H. Kleinschmidt, „An analytical model for multihop LoRaWAN networks”, *Internet of Things*, köt. 22, o. 100807, júl. 2023, doi: 10.1016/j.iot.2023.100807.

[64] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, és A. Chehab, „LoRaWAN security survey: Issues, threats and possible mitigation techniques”, *Internet of Things*, köt. 12, o. 100303, dec. 2020, doi: 10.1016/j.iot.2020.100303.

[65] L. Febriarti, A. M. Imammuddin, és D. Suprianto, „Analysis of Coverage Range and Data Transmission Success Rate of LoRaWAN in the Implementation of an Electrical Power Monitoring System”, *JURNAL JARTEL: Jurnal Jaringan Telekomunikasi*, köt. 15, sz. 4, o. 479–484, dec. 2025, doi: 10.33795/jartel.v15i4.8716.

[66] M. Mehic, M. Duliman, N. Selimovic, és M. Voznak, „LoRaWAN End Nodes: Security and Energy Efficiency Analysis”, *Alexandria Engineering Journal*, köt. 61, sz. 11, o. 8997–9009, nov. 2022, doi: 10.1016/j.aej.2022.02.035.

[67] Semtech, *AN1200.22 LoRa Modulation Basics*. 2015. Elérés: 2021. november 10. [Online]. Elérhető: https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/2R0000001OJu/xvKUc5w9yjG1q5Pb2IIkpolW54YYqGb.frOZ7HQBcRc

[68] LoRa Alliance, *RP002-1.0.4 Regional Parameters*. 2022. Elérés: 2025. március 2. [Online]. Elérhető: https://resources.lora-alliance.org/technical-specifications/rp002-1-0-4-regional-parameters

[69] P. Maurya, A. Singh, és A. A. Kherani, „A review: spreading factor allocation schemes for LoRaWAN”, *Telecommun. Syst.*, köt. 80, sz. 3, o. 449–468, júl. 2022, doi: 10.1007/s11235-022-00903-4.

[70] D. Borsos, „Image Transmission with LoRaWAN in Agriculture”, in *Critical Infrastructure Protection in the Light of the Armed Conflicts. HCC 2022. Advanced Sciences and Technologies for Security Applications*, T. A. Kovács, Z. Nyikes, T. Berek, N. Daruka, és L. Tóth, Szerk., Cham: Springer, 2024, o. 235–246. doi: 10.1007/978-3-031-47990-8_21.

[71] A. H. Jebril és R. A. Rashid, „A systematic literature review on downlink frames in LoRaWAN”, *Computers and Electrical Engineering*, köt. 101, o. 108006, júl. 2022, doi: 10.1016/j.compeleceng.2022.108006.

[72] D. Borsos, „Development and Optimisation of Exit Procedures for LoRaWan Nodes”, in *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, szept. 2024, o. 000523–000527. doi: 10.1109/SISY62279.2024.10737616.

[73] D. Fernandes Carvalho *és mtsai.*, „A test methodology for evaluating architectural delays of LoRaWAN implementations”, *Pervasive Mob. Comput.*, köt. 56, o. 1–17, máj. 2019, doi: 10.1016/j.pmcj.2019.03.002.

[74] D. Borsos, „APPLICATIONS OF LORAWAN TECHNOLOGY”, *CYBER SECURITY REVIEW online*, o. 1–6, 2020, Elérés: 2024. május 22. [Online]. Elérhető: https://www.cybersecurity-review.com/wp-content/uploads/2020/09/Doniz-Borsos-article-APPLICATIONS-OF-LORAWAN-TECHNOLOGY-Cyber-Security-Review-Online.pdf

[75] L. Berek, *Biztonságtechnika*. Budapest, Magyarország: Nemzeti Közszolgálati Egyetem (NKE), 2014. Elérés: 2020. december 2. [Online]. Elérhető: https://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf

[76] L. Berek, T. Berek, és L. Berek, *Személy- és vagyonbiztonság*. Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2016. Elérés: 2025. március 2. [Online]. Elérhető: https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/32978/3071%20Szem%c3%a9ly-%20%c3%a9s%20vagyonbiztons%c3%a1g.pdf?sequence=1&isAllowed=y

[77] R. Pető és D. Tokody, „Building and Operating a Smart City”, *Interdisciplinary Description of Complex Systems*, köt. 17, sz. 3, o. 476–484, 2019, doi: 10.7906/indecs.17.3.6.

[78] C. Ucar, M. Maloku, O. Yugay, és D. Budimir, „IoT Motion Detection Sensors for Monitoring in a Smart Campus”, in *2024 13th Mediterranean Conference on Embedded Computing (MECO)*, IEEE, jún. 2024, o. 1–4. doi: 10.1109/MECO62516.2024.10577922.

[79] S. Satpathy, B. Sahoo, és A. K. Turuk, „Sensing and Actuation as a Service Delivery Model in Cloud Edge centric Internet of Things”, *Future Generation Computer Systems*, köt. 86, o. 281–296, szept. 2018, doi: 10.1016/j.future.2018.04.015.

[80] V. Bonilla, B. Campoverde, és S. G. Yoo, „A Systematic Literature Review of LoRaWAN: Sensors and Applications”, *Sensors*, köt. 23, sz. 20, o. 8440, okt. 2023, doi: 10.3390/s23208440.

[81] L. Berek, „Óbuda University e-Bulletin”, *ÓBUDA UNIVERSITY E-BULLETIN*, köt. 6, sz. 1, o. 172–20, 2016, Elérés: 2025. szeptember 7. [Online]. Elérhető: https://uni-obuda.hu/e-bulletin/Berek_7.pdf

[82] GSMA, *The Mobile Economy 2024*. 2024. Elérés: 2026. január 4. [Online]. Elérhető: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf

[83] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, és J. H. Reed, „LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation”, *IEEE Communications Magazine*, köt. 54, sz. 4, o. 54–61, ápr. 2016, doi: 10.1109/MCOM.2016.7452266.

[84] D. Borsos, „Additional wireless communication technologies that are used in LoRaWAN products and their importance in the field of personal and property protection”, in *XXXVI. Kandó Konferencia 2020*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 121–130.

[85] H. Boyes, B. Hallaq, J. Cunningham, és T. Watson, „The industrial internet of things (IIoT): An analysis framework”, *Comput. Ind.*, köt. 101, o. 1–12, okt. 2018, doi: 10.1016/j.compind.2018.04.015.

[86] H. Bhatia, S. N. Panda, és D. Nagpal, „Internet of Things and its Applications in Healthcare-A Survey”, in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, IEEE, jún. 2020, o. 305–310. doi: 10.1109/ICRITO48877.2020.9197816.

[87] M. Szántó *és mtsai.*, „Developing a Health Support System to Promote Care for the Elderly”, *Sensors*, köt. 25, sz. 2, o. 455, 2025, doi: 10.3390/s25020455.

[88] H. Ali Hashim, S. L. Mohammed, és S. K. Gharghan, „Accurate fall detection for patients with Parkinson’s disease based on a data event algorithm and wireless sensor nodes”, *Measurement*, köt. 156, o. 107573, máj. 2020, doi: 10.1016/j.measurement.2020.107573.

[89] P. Battistoni, M. Sebillo, és G. Vitiello, „An IoT-Based Mobile System for Safety Monitoring of Lone Workers”, *IoT*, köt. 2, sz. 3, o. 476–497, aug. 2021, doi: 10.3390/iot2030024.

[90] T. Hadwen, V. Smallbon, Q. Zhang, és M. D’Souza, „Energy efficient LoRa GPS tracker for dementia patients”, in *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, IEEE, júl. 2017, o. 771–774. doi: 10.1109/EMBC.2017.8036938.

[91] D. Borsos, „LoRaWAN Certified Product Trends with a Special Focus on Smart Cities and Property Protection”, *Interdisciplinary Description of Complex Systems*, köt. 23, sz. 3, o. 230–239, 2025, doi: 10.7906/indecs.23.3.4.

[92] LoRa Alliance, „LoRaWAN Certified”. Elérés: 2025. február 6. [Online]. Elérhető: https://lora-alliance.org/lorawan-certification/

[93] LoRa Alliance, „LoRaWAN® Marketplace”. Elérés: 2025. december 6. [Online]. Elérhető: https://lora-alliance.org/marketplace/search/?mp_certified=1

[94] D. Borsos és L. Berek, „Challenges of LoRaWAN technology in smart city solutions”, *Interdisciplinary Description of Complex Systems*, köt. 20, sz. 1, o. 1–10, febr. 2022, doi: 10.7906/indecs.20.1.1.

[95] H. E. Elbsir, M. Kassab, S. Bhiri, és M. H. Bedoui, „Evaluation of LoRaWAN class B performances and its optimization for better support of actuators”, *Comput. Commun.*, köt. 198, o. 128–139, jan. 2023, doi: 10.1016/j.comcom.2022.11.016.

[96] D. Borsos és L. Berek, „Jelenlétdetektálás megoldásai és személy- és vagyonvédelmi aspektusai”, in *KVK Habilitációs és PhD Workshop Minikonferencia: Kiadvány kötet*, T. Wührl, Szerk., Budapest, Magyarország: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2024, o. 118–124.

[97] MSZ EN 50131-x-x Szabványsorozat, *Riasztórendszerek. Behatolás- és támadásjelző rendszerek.*

[98] MSZ EN IEC 62676-x-x Szabványsorozat, *Video-megfigyelőrendszerek biztonsági alkalmazásokhoz.*

[99] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. 2022.

[100] MSZ CLC IEC/TS 62443-x-x Szabványsorozat, „Ipari automatizálási és szabályozási rendszerek biztonsága."

[101] D. BORSOS, Á. KOHANECZ, és D. KOZMA, „LoRa and LoRaWAN Tests in the Aspect of Critical Infrastructures", *TRANSACTIONS of the VŠB – Technical University of Ostrava Safety Engineering Series*, köt. 17, sz. 1, o. 1–11, jún. 2022, doi: 10.35182/tses-2022-0001.

[102] D. Borsos, „Applications of LoRaWAN technology", in *ICCECIP 2019 Abstract book*, Z. Nyikes, Szerk., Budapest, Hungary: Óbudai Egyetem, 2019, o. 22.

[103] D. M. Kozma, Á. Kohanecz, és D. Borsos, „LoRaWAN hálózat stabilitás vizsgálata különböző környezeti viszonyok mellett", in *XXXVII. Kandó Konferencia*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2021, o. 41–50.

[104] D. Borsos, „Traffic-Based Anomaly Detection in LoRaWAN Networks under Indoor Environment", in *2025 IEEE 23rd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, szept. 2025, o. 000357–000362. doi: 10.1109/SISY67000.2025.11205375.

[105] D. BORSOS, „Lorawan Solutions in the COVID-19 Aspect", *TRANSACTIONS of the VŠB – Technical University of Ostrava Safety Engineering Series*, köt. 16, sz. 1, 2021, doi: 10.35182/tses-2021-0002.

[106] R. Roman, J. Zhou, és J. Lopez, „On the features and challenges of security and privacy in distributed internet of things", *Computer Networks*, köt. 57, sz. 10, o. 2266–2279, júl. 2013, doi: 10.1016/j.comnet.2012.12.018.

[107] S. Sicari, A. Rizzardi, L. A. Grieco, és A. Coen-Porisini, „Security, privacy and trust in Internet of Things: The road ahead”, *Computer Networks*, köt. 76, o. 146–164, jan. 2015, doi: 10.1016/j.comnet.2014.11.008.

[108] M. El-Hosseini, H. ZainEldin, H. Arafat, és M. Badawy, „A fire detection model based on power-aware scheduling for IoT-sensors in smart cities with partial coverage”, *J. Ambient Intell. Humaniz. Comput.*, köt. 12, sz. 2, o. 2629–2648, febr. 2021, doi: 10.1007/s12652-020-02425-w.

[109] M. Beyrouti, A. Lounis, B. Lussier, A. Bouabdallah, és A. E. Samhat, „Vulnerability-oriented risk identification framework for IoT risk assessment”, *Internet of Things*, köt. 27, o. 101333, okt. 2024, doi: 10.1016/j.iot.2024.101333.

[110] D. Borsos, Á. Kohanecz, és D. M. Kozma, „Lorawan networks test aspects of critical infrastructures”, in *ICCECIP 2021 - Poster*, Budapest, Hungary: Óbudai Egyetem, 2021, o. 1.

[111] Antenna Hungária, „Az Antenna Hungária fejlesztők részére megnyitotta országos IoT hálózatát”. Elérés: 2023. augusztus 6. [Online]. Elérhető: https://4igtavkozlesiholding.hu/hu/hirek/az-antenna-hungaria-fejlesztok-reszere-megnyitotta-orszagos-iot-halozatat

[112] A. H. Jebril, A. Sali, A. Ismail, és M. F. A. Rasid, „Overcoming Limitations of LoRa Physical Layer in Image Transmission”, *Sensors*, köt. 18, sz. 10, o. 3257, szept. 2018, doi: 10.3390/s18103257.

[113] D. Borsos, „Lorawan Picture Transmission Solutions in Agriculture”, in *ICCECIP 2022 4th International Conference on Central European Critical Infrastructure Protection: Abstract Book*, Z. Nyikes és T. A. Kovács, Szerk., Budapest, Hungary: Óbudai Egyetem, 2022, o. 38.

[114] T. Chen, D. Eager, és D. Makaroff, „Efficient Image Transmission Using LoRa Technology In Agricultural Monitoring IoT Systems”, in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, júl. 2019, o. 937–944. doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00166.

[115] J. M. Marais, R. Malekian, és A. M. Abu-Mahfouz, „LoRa and LoRaWAN testbeds: A review”, in *2017 IEEE AFRICON*, IEEE, szept. 2017, o. 1496–1501. doi: 10.1109/AFRCON.2017.8095703.

[116] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*. 2022.

[117] F. A. Alaba, M. Othman, I. A. T. Hashem, és F. Alotaibi, „Internet of Things security: A survey”, *Journal of Network and Computer Applications*, köt. 88, o. 10–28, jún. 2017, doi: 10.1016/j.jnca.2017.04.002.

[118] M. Ammar, G. Russello, és B. Crispo, „Internet of Things: A survey on the security of IoT frameworks”, *Journal of Information Security and Applications*, köt. 38, o. 8–27, febr. 2018, doi: 10.1016/j.jisa.2017.11.002.

[119] J. Bugeja, A. Jacobsson, és P. Davidsson, „On Privacy and Security Challenges in Smart Connected Homes”, in *2016 European Intelligence and Security Informatics Conference (EISIC)*, IEEE, aug. 2016, o. 172–175. doi: 10.1109/EISIC.2016.044.

[120] L. Catarinucci *és mtsai.*, „An IoT-Aware Architecture for Smart Healthcare Systems”, *IEEE Internet Things J.*, köt. 2, sz. 6, o. 515–526, dec. 2015, doi: 10.1109/JIOT.2015.2417684.

[121] J. Zhou, Z. Cao, X. Dong, és A. V. Vasilakos, „Security and Privacy for Cloud-Based IoT: Challenges”, *IEEE Communications Magazine*, köt. 55, sz. 1, o. 26–33, jan. 2017, doi: 10.1109/MCOM.2017.1600363CM.

[122] Y. Meidan *és mtsai.*, „N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders”, *IEEE Pervasive Comput.*, köt. 17, sz. 3, o. 12–22, júl. 2018, doi: 10.1109/MPRV.2018.03367731.

[123] E. Dritsas és M. Trigka, „A Survey on Cybersecurity in IoT”, *Future Internet*, köt. 17, sz. 1, o. 30, jan. 2025, doi: 10.3390/fi17010030.

[124] P. D. More, S. R. Sakhare, és P. Mahalle, „Identity Management in the Internet of Things: A Survey of the State of the Art”, *IEEE Syst. Man Cybern. Mag.*, köt. 9, sz. 4, o. 13–19, okt. 2023, doi: 10.1109/MSMC.2022.3230215.

[125] IoT Security Foundation, „IoT Cybersecurity for Facilities Professionals in the Smart Built Environment”. Elérés: 2024. április 4. [Online]. Elérhető:

https://iotsecurityfoundation.org/wp-content/uploads/2023/03/IoT-Cybersecurity-for-Facilities-Professionals-in-the-Smart-Built-Environment-RELEASE-1-0-FINAL-30-03-2023.pdf

[126] IoT Security Foundation, *Secure Design - Best Practice Guides*. 2019. Elérés: 2024. április 4. [Online]. Elérhető: https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf

[127] N. Yousefnezhad, A. Malhi, és K. Främling, „Security in product lifecycle of IoT devices: A survey”, *Journal of Network and Computer Applications*, köt. 171, o. 102779, dec. 2020, doi: 10.1016/j.jnca.2020.102779.

[128] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, és T. Watteyne, „Understanding the Limits of LoRaWAN”, *IEEE Communications Magazine*, köt. 55, sz. 9, o. 34–40, 2017, doi: 10.1109/MCOM.2017.1600613.

[129] J. Haxhibeqiri, E. De Poorter, I. Moerman, és J. Hoebeke, „A Survey of LoRaWAN for IoT: From Technology to Application”, *Sensors*, köt. 18, sz. 11, o. 3995, nov. 2018, doi: 10.3390/s18113995.

[130] D. Maccarrone, „10 IoT Trends Shaping the Future in 2025”, LORIOT. Elérés: 2026. február 6. [Online]. Elérhető: https://loriot.io/blog/IoT-trends-2025.html

RÖVIDÍTÉSJEGYZÉK

Rövidítés	Angol nyelvű kifejezés	Magyar nyelvű kifejezés
3GPP	3rd Generation Partnership Project	Harmadik Generációs Partnerségi Projekt
ABP	Activation By Personalization	Előre konfigurált kulcsokkal történő aktiválás
ADR	Adaptive Data Rate	Adaptív adatsebesség-szabályozás
BW	Bandwidth	Sávszélesség
CCTV	Closed Circuit Television	Zártláncú televíziós rendszer
CR	Coding Rate	Kódolási ráta
CSS	Chirp Spread Spectrum	Chirp alapú szórt spektrumú moduláció
DR	Data Rate	Adatráta
EU	Europe	Európa
FCnt	Frame Counter	Keretszámláló
GPS	Global Positioning System	Globális helymeghatározó rendszer
ICT	Information and Communications Technology	Információs- és kommunikációs technológiák
IoT	Internet of Things	Dolgok Internete.
IP	Internet Protocol	Internetprotokoll
ISM	Industrial, Scientific and Medical	Ipari, tudományos és orvosi
IT	Information Technology	Információs technológiák
LPWAN	Low Power Wide Area Network	Alacsony energiafogyasztású, nagy kiterjedésű hálózatok
LTE	Long Term Evolution	Hosszú távú evolúciójú mobilhálózati technológia
Max.	Maximum	Maximum
Min.	Minimum	Minimum
MPLR	Multi-Packet LoRa	Többcsomagos LoRa kommunikáció
OTAA	Over-The-Air Activation	Rádiós csatornán keresztüli aktiválás
PCB	Printed Circuit Board	Nyomtatott áramkör
PCBA	Printed Circuit Board Assembly	Összeszerelt nyomtatott áramköri lap
PER	Package Error Rate	Csomagvesztési arány
QoS	Quality of Service	Szolgáltatásminőség
RF	Radio Frequency	Rádiófrekvencia
RFID	Radio Frequency Identification	Rádiófrekvenciás azonosítás
RSSI	Received Signal Strength Indicator	Vett jel erősségét jelző mutató
SF	Spreading Factor	Terjedési tényező
SNR	Signal-to-noise ratio	Jel-zaj viszony
ToA	Time on Air	Levegőben töltött idő (adásidő)

2. ábra vonatkozó régióinak rövidítésjegyzéke:

Régió	Angolul	Magyarul
AS	Asia	Ázsiai régióra definiált LoRaWAN frekvenciasáv (AS923)
AU	Australia	Ausztráliai LoRaWAN frekvenciasáv (AU915)
CN	China	Kínai LoRaWAN frekvenciasáv (CN470 / CN779)
EU	Europe	Európai LoRaWAN frekvenciasáv (EU868/EU433)
IN	India	Indiai LoRaWAN frekvenciasáv (IN865)
KR	Korea	Dél-koreai LoRaWAN frekvenciasáv (KR920)
RU	Russia	Oroszországi LoRaWAN frekvenciasáv (RU864)
US	United States	Amerikai LoRaWAN frekvenciasáv (US915)

3. táblázathoz tartozó azonosítók és kulcsok jegyzéke:

Azonosító/Kulcs	Angolul	Magyarul
AppEUI	Application identifier	Alkalmazás azonosító
AppKey	Application key	Alkalmazáskulcs
AppSKey	Application session key	Alkalmazás munkamenet kulcs
DevAddr	End-device address	Végberendezés hálózati azonosító címe
DevEUI	End-device identifier	Végberendezés globális, egyedi azonosítója
FNwkSIntKey	Forwarding Network session integrity key	Végberendezés hálózati munkamenet kulcsa
JoinEUI	Join-Server identifier	Végberendezés join-szerver azonosítója
NwkKey	Network Key	Hálózati kulcs
NwkSEncKey	Network session encryption key	Hálózati munkamenet titkosítási kulcs
NwkSKey	Network session key	Hálózati munkamenet kulcs
SNwkSIntKey	Serving Network session integrity key	Kiszolgáló hálózat munkamenet-integritási kulcsa

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

KÖSZÖNETNYILVÁNÍTÁS

Szeretném köszönetemet kifejezni mindazoknak, akik hozzájárultak tanulmányaimhoz és kutatásom megvalósításához.

Kiemelten köszönöm témavezetőmnek a szakmai iránymutatást, a hasznos tanácsokat és a folyamatos támogatást.

Köszönöm az intézmény munkatársainak és kollégáimnak a közreműködésüket és segítségüket.

Végül köszönöm családomnak és barátaimnak a türelmet és a folyamatos támogatást.