DR.VARGA PÉTER JÁNOS
EGYETEMI DOCENS

A vezeték nélküli lokális hálózatok biztonsága

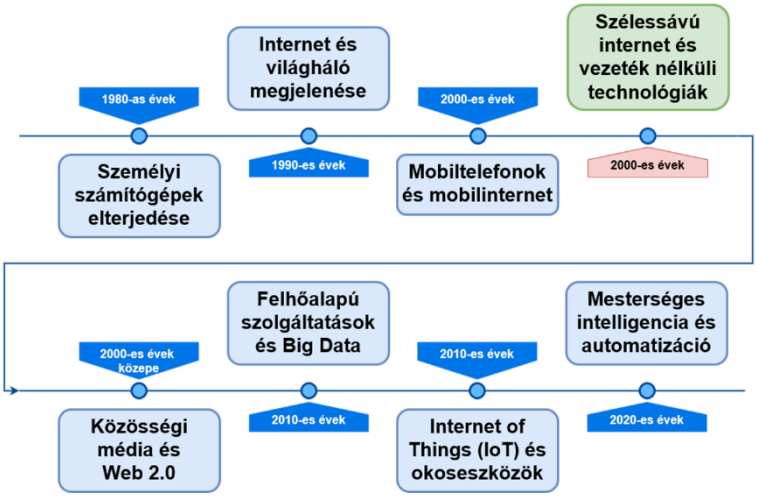
Tartalom

1 A kutatás előzményei

A PhD-fokozat megszerzését követően kutatási tevékenységem több, egymással szorosan összefüggő területre terjedt ki, amelyek közül meghatározó szerepet játszott a vezeték nélküli kommunikációs hálózatok vizsgálata. E kutatási irány szerves folytatását képezte a doktori képzés során megkezdett munka, amely a vezeték nélküli lokális hálózatok (WLAN) technológiai fejlődésére és biztonsági kérdéseire fókuszált. A vizsgálatok középpontjában már ekkor az a kérdés állt, hogy a WLAN-hálózatok széles körű elterjedése miként formálja át a digitális társadalom infrastruktúráját, és ezzel párhuzamosan milyen új technológiai és biztonsági kihívások jelennek meg [1].

A kutatások korai szakaszában egyértelművé vált, hogy a vezeték nélküli hálózatok biztonságát nem elegendő kizárólag technikai vagy felhasználói oldalról megközelíteni. A WLAN-hálózatok tömeges megjelenése olyan infrastruktúrát hozott létre, amely szorosan összekapcsolódik a digitális társadalom működésével, így biztonsági kérdései szükségszerűen túlmutatnak az egyedi hálózatok vagy eszközök szintjén. A probléma értelmezése ezért társadalmi és infrastrukturális dimenziót is igényel.

A digitális társadalom kialakulása a 20. század végén és a 21. század elején gyorsult fel, amikor az információs és kommunikációs technológiák fejlődése alapvetően átalakította a társadalmi és gazdasági struktúrákat [2]. Az internet tömeges elérhetősége, a mobilkommunikáció elterjedése, valamint a hálózati és számítástechnikai eszközök mindennapivá válása új működési mintákat hozott létre mind a lakossági, mind a vállalati és intézményi környezet számára. A digitális társadalom kialakulásának főbb mérföldköveit a 20. század végétől napjainkig az következő ábra szemlélteti.



1. ábra: A digitális társadalom kialakulásának mérföldkövei

Jelen kutatásom elsősorban a 2000-es évek elején megjelenő, és azóta folyamatosan fejlődő vezeték nélküli lokális hálózatok városi környezetben jelentkező biztonsági kockázatainak és védelmi jellemzőinek empirikus, idősoros vizsgálatára koncentrál. Az ilyen típusú hálózatok felhasználói – magánszemélyek, vállalkozások, kormányzati és önkormányzati szervek, valamint különböző civil és oktatási intézmények – eltérő módon és eltérő időben kapcsolódtak be a vezeték nélküli hálózatok használatába. A WLAN-technológia fejlődése során ezek a szereplők különböző ütemben és eltérő műszaki és biztonsági felkészültséggel adaptálták az új megoldásokat, ami heterogén hálózati környezetet eredményezett.

A kutatás kezdeti szakaszában az IEEE 802.11 szabványcsalád fejlődésének elemzése került előtérbe, különös tekintettel a 802.11n, 802.11ac és 802.11ax szabványváltozatokra (Wi-Fi 4, Wi-Fi 5 és Wi-Fi 6) [3]. A vizsgálatok célja annak feltárása volt, hogy a szabványfejlődés milyen új műszaki képességeket, valamint milyen biztonsági mechanizmusokat vezetett be, és ezek miként jelennek meg a gyakorlati implementációkban. Az elméleti megalapozást a nemzetközi WLAN-szabványosítás folyamata, valamint a városi digitális infrastruktúrák térbeli és technológiai eloszlásának vizsgálata adta.

Ezt az elméleti keretet fokozatosan egészítettem ki valós környezetben végzett mérésekkel. 2012-től kezdődően egy hosszú távú, egységes metodikára épülő vizsgálati sorozatot végeztem Budapest területén, amelynek célja a vezeték nélküli hálózatok sűrűségének, technológiai megoszlásának és biztonsági jellemzőinek feltérképezése volt. A kijelölt vizsgálati útvonal mintegy 33 km hosszúságú, és lefedte a főváros különböző városszerkezeti zónáit, beleértve a lakótelepi, családi házas, ipari, valamint bel- és külvárosi területeket. Az eltérő karakterű környezetek bevonása lehetővé tette a WLAN-hálózatok összehasonlítható vizsgálatát különböző infrastrukturális és társadalmi kontextusokban.

A terepi adatgyűjtéshez kialakított vizsgálati környezet standardizált hardver- és szoftverelemekre épült. A mérések során alkalmazott konfiguráció lehetővé tette a WLAN-hálózatok azonosítását, a mérés pozíciója mellé a jelszintek, a csatornakiosztás, az alkalmazott titkosítási eljárások és a szabványváltozatok rögzítését. A GPS-alapú helymeghatározás révén minden mérési adat térbeli koordinátával egészült ki, ami megteremtette a hálózati végpontok térképi alapú és idősoros elemzésének lehetőségét. A vizsgálati eredményeket

rendszeresen összevetettem a Wireless Geographic Logging Engine (WIGLE) nyilvános adatbázisával, biztosítva az adatok ellenőrizhetőségét és nemzetközi összehasonlíthatóságát.

A kutatás fókusza 2018-tól tovább bővült, igazodva a hazai hozzáférési infrastruktúra átalakulásához [4]. A Szupergyors Internet Program hatására jelentősen nőtt a nagy sávszélességű vezetékes hozzáférések aránya, valamint elterjedtek a korszerű, Wi-Fi 5 és Wi-Fi 6 kompatibilis, integrált WLAN-funkcióval rendelkező végberendezések [5]. A Központi Statisztikai Hivatal (KSH) és a Nemzeti Média- és Hírközlési Hatóság (NMHH) által publikált adatokban megjelenő trendeket a saját mérések is alátámasztották, lehetővé téve a technológiai és üzemeltetési változások empirikus vizsgálatát [6, 7].

A 2012 és 2024 közötti időszakban végzett ismételt mérések eredményeként egy folyamatosan bővülő adatbázis jött létre, amely alkalmas a WLAN-hálózatok hosszú távú technológiai átmeneteinek és biztonsági állapotának elemzésére.

Az egységes vizsgálati metodika lehetővé tette egy többdimenziós elemzési keret kialakítását, amely technológiai, biztonsági és társadalmi szempontból egyaránt értelmezi a vezeték nélküli infrastruktúra fejlődését. Ez a megközelítés hazai viszonylatban újszerűnek tekinthető. A kutatás

eredményei több hazai és nemzetközi tudományos közleményben jelentek meg, valamint közvetlenül hasznosultak az egyetemi oktatásban, különösen a vezeték nélküli kommunikációval és hálózatbiztonsággal foglalkozó kurzusok tananyagában.

A kutatási eredmények egy egységes, hosszú távú vizsgálati sorozat részét képezik, amely a városi WLAN-infrastruktúra biztonsági jellemzőit módszertanilag kontrollált környezetben vizsgálja.

2 Új tudományos eredmények

Eredményeim és azok alátámasztását rendszerezetten három alfejezetpontban mutatom be:

- A városi WLAN-környezet biztonsági jellemzőinek idősoros vizsgálata ütemezett wardriving mérésekkel;
- A városi WLAN-végpontok biztonsági paramétereinek idősoros és térbeli elemzése;
- Szolgáltatói integrált WLAN-funkcióval rendelkező végberendezések elterjedésének biztonsági hatásai városi környezetben.

2.1 A városi WLAN-környezet biztonsági jellemzőinek idősoros vizsgálata ütemezett wardriving mérésekkel

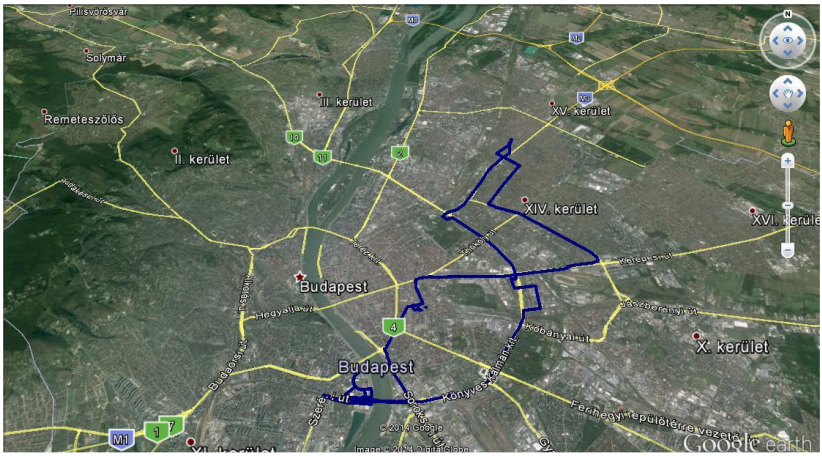
Tézis 1: Bebizonyítottam, hogy egy városi környezetben kijelölt vizsgálati útvonal mentén végzett, ütemezett wardriving mérések révén olyan hosszú idősoros adatbázis állítható elő, amely reprodukálható módon alkalmas a vezeték nélküli lokális hálózati végpontok eloszlásának és biztonsági jellemzőinek

elemzésére, miközben az adatgyűjtés kizárólag a nyilvánosan sugárzott hálózati jellemzőkre korlátozódik. [V1, V2, V3, V4]

Az ütemezett wardriving mérésekre épülő adatgyűjtési módszertan

A vezeték nélküli lokális hálózatok városi környezetben történő vizsgálata különösen összetett feladat, mivel a végpontok telepítése decentralizált, az üzemeltetési gyakorlatok heterogének, és a hálózati infrastruktúra dinamikusan változik. A kutatásaim kiindulópontja az volt, hogy a WLAN-környezet biztonsági állapotáról csak akkor lehet érdemi következtetéseket levonni, ha az adatgyűjtés nem eseti jellegű, hanem időben és térben kontrollált, hosszú távon is fenntartható módon történik.

Ennek érdekében egy ütemezett wardriving módszertanra épülő mérési keretrendszert dolgoztam ki, amelynek központi eleme egy előre definiált, városi környezetet reprezentáló 33 kilométeres vizsgálati útvonal. A kijelölt útvonal lakóövezeti, ipari, irodai és vegyes funkciójú területeket egyaránt érint, így alkalmas arra, hogy különböző telepítési és üzemeltetési gyakorlatok egyidejűleg jelenjenek meg a mérési adatokban. A következő ábra a vizsgálat útvonalát szemlélteti.



2. ábra: A vizsgálat útvonala

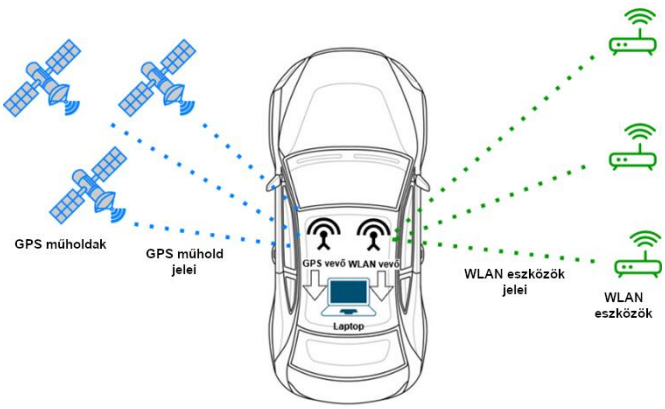
Az útvonal állandósága nem pusztán a reprodukálhatóságot szolgálta, hanem lehetővé tette azt is, hogy az egymást követő mérési ciklusok közötti különbségek elsősorban időbeli és technológiai változásokra, ne pedig térbeli eltérésekre legyenek visszavezethetők. A mérések minden esetben hasonló napszakban történtek, csökkentve a forgalmi és terhelési viszonyokból fakadó torzításokat.

A méréseket 2012 és 2024 között minden évben, az év azonos időszakában végeztem el, biztosítva ezzel a szezonális hatások minimalizálását és az idősoros összehasonlíthatóságot. A vezeték nélküli hálózatok működését rövid távon számos külső tényező befolyásolhatja, így például az időjárási viszonyok, az

oktatási és munkarendhez kapcsolódó ciklusok, valamint az ideiglenes rendezvényekhez kötődő hálózati végpontok megjelenése. Az éves mérések azonos időszakra történő időzítése lehetővé tette, hogy ezek a hatások az idősoros elemzések során kiegyenlítődjenek, és a megfigyelt változások elsősorban technológiai fejlődésre vagy üzemeltetési gyakorlatok módosulására legyenek visszavezethetők. A módszertan egyik lényegi eleme az volt, hogy a WLAN-környezetet idősoros rendszerként kezeltem, nem pedig statikus infrastruktúraként.

A vizsgálati környezet és a rögzített biztonsági jellemzők

A mérési rendszer hardveres és szoftveres felépítése kifejezetten a passzív adatgyűjtést támogatta. A használt WLAN-adapter és mérőszoftver kizárólag a 802.11 szabványcsalád által definiált beacon frame-ekből származó információkat rögzítették. Aktív asszociáció, forgalomgenerálás vagy hitelesítési kísérlet nem történt, így a mérési eljárás nem befolyásolta a vizsgált hálózatok működését. A következő ábra a mérőrendszer felépítését szemlélteti.



3. ábra: A mérőrendszer felépítése

A mérőrendszer főbb elemei a:

- GPS vevőkészülék,
- WLAN kártya,
- az adatrögzítő laptop.

A rögzített paraméterek körét tudatosan úgy választottam meg, hogy azok csoportosítva alkalmasak legyenek a WLAN-környezet biztonsági állapotának jellemzésére. Ezek közé tartoztak különösen:

- az SSID azonosítók,
- az alkalmazott 802.11 szabványverzió,
- a működési frekvenciasáv és csatorna,

- a titkosítási és autentikációs mechanizmus típusa,
- a hozzáférési pont gyártójára utaló információk.

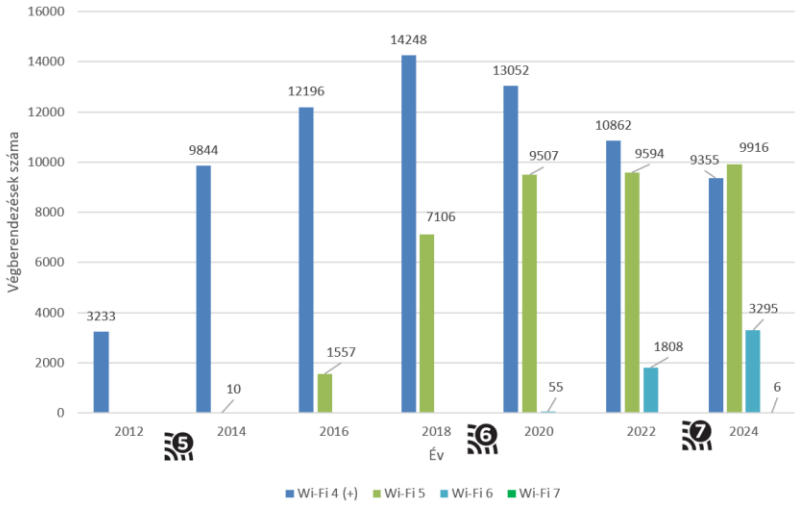
Ezek a jellemzők egyenként nem adnak teljes képet egy hálózat biztonságáról, azonban nagy elemszám mellett, idősoros bontásban alkalmasak arra, hogy a biztonsági gyakorlat változásait leírják.

Idősoros adatfeldolgozás és külső adatforrásokkal történő validálás

Az adatfeldolgozás során kiemelt szerepet kapott az idősoros normalizáció. A mérési ciklusok során rögzített végpontszám folyamatosan növekedett, ezért az abszolút darabszámok önmagukban nem voltak alkalmasak összehasonlításra. Az elemzések így relatív megoszlásokra, arányokra és trendekre épültek, különösen a titkosítási mechanizmusok és a szabványgenerációk tekintetében [8].

A hosszú idősoros adatbázis lehetővé tette annak vizsgálatát is, hogy az újabb technológiák megjelenése milyen ütemben szorítja ki a korábbi megoldásokat, illetve hogy a technológiai fejlődés együtt jár-e a biztonsági konfigurációk javulásával. A mérések azt mutatták, hogy bár az újabb szabványok - például

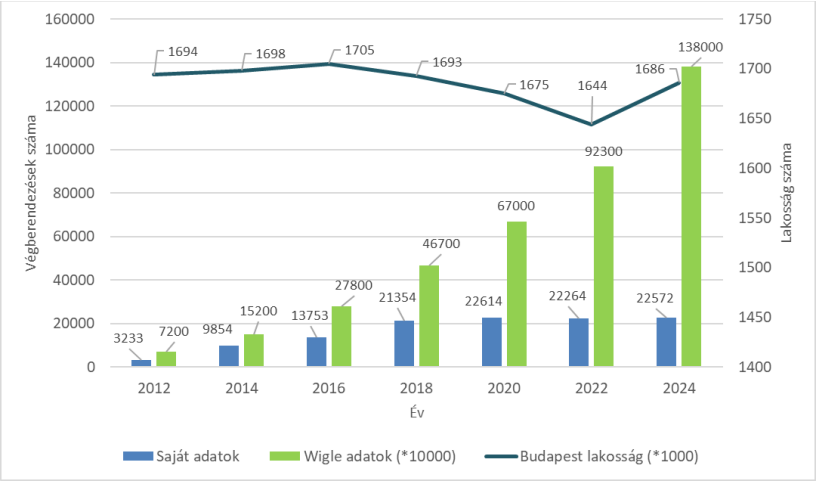
802.11ac, 802.11ax - fokozatosan dominánssá váltak, a régebbi konfigurációk hosszabb ideig fennmaradtak a városi környezetben. Ezt jól szemlélteti a következő ábra, mely a Wi-Fi 4 / Wi-Fi 5 / Wi-Fi 6 végpontok darabszámának alakulását mutatja be 2012 és 2024 között.



4. ábra: Wi-Fi 4 / Wi-Fi 5 / Wi-Fi 6 végpontok arányának változása időben

A módszertan validálása érdekében az általam gyűjtött adatokat több külső adatforrással is összevetettem. Különösen fontos referencia volt a WIGLE (Wireless Geographic Logging Engine) nyilvános adatbázisa, amely globális léptékben tartalmaz WLAN-végpontokra vonatkozó információkat [9]. A

saját mérések és a WIGLE-adatok együttes megjelenítése mellett az összehasonlító ábrákon a Központi Statisztikai Hivatal (KSH) Budapest lakosságára vonatkozó idősoros adatai is szemléltetésre kerültek, lehetőséget teremtve arra, hogy a vezeték nélküli hálózati végpontok számának változását demográfiai kontextusban is értelmezzem [6]. Az összevetés célja nem oksági kapcsolat igazolása volt, hanem annak bemutatása, hogy a mérési adatok által kirajzolt trendek nem elszigetelt technológiai jelenségek, hanem a városi környezet strukturális átalakulásával párhuzamosan jelennek meg. Ezeket az adatokat szemlélteti a következő ábra.



5. ábra: Saját wardriving mérések, WIGLE-adatok és a KSH Budapest lakosságára vonatkozó idősoros adatainak együttes ábrázolása

Az ábra alapján megállapítható, hogy a KSH adatai szerint Budapest lakosságának száma 2016 és 2022 között csökkenő tendenciát mutatott, amellyel időben egybeesik a saját WLAN-mérésekben 2022-ben tapasztalt végpontszám visszaeséssel.

Fontos hangsúlyozni, hogy a vizsgálati módszerem tudatosan nem törekedett a WLAN-hálózatok teljes körű biztonsági auditjára (ilyen kísérlet sorozat jogi kérdéseket is felvetne). A cél nem egyedi hálózatok sebezhetőségének feltárása volt, hanem a városi WLAN-környezet aggregált, statisztikai jellemzése. Ebből a szempontból a nyilvánosan sugárzott jellemzők elegendő információt szolgáltattak a biztonsági állapot trendalapú elemzéséhez, miközben a mérési eljárás jogi és etikai szempontból is fenntartható maradt.

Az ütemezett wardriving mérésekre épülő módszertan lehetővé tette egy olyan hosszú idősoros adatbázis kialakítását, amely reprodukálható módon írja le a vezeték nélküli lokális hálózati végpontok eloszlását és alapvető biztonsági jellemzőit egy városi környezetben. Ez az adatbázis szolgált alapul a későbbi tézisekben bemutatott biztonsági mintázatok és technológiai hatások elemzéséhez.

Részösszegzés

Az első tézisben bemutatott kutatási eredmények alapján megállapítható, hogy a városi vezeték nélküli lokális hálózatok vizsgálata csak akkor vezet megbízható és általánosítható következtetésekhez, ha az adatgyűjtés hosszú távon következetes, térben kontrollált és időben reprodukálható módon történik. Az ütemezett wardriving mérésekre épülő módszertan alkalmazása lehetővé tette egy olyan idősoros adatbázis kialakítását, amely túlmutat az eseti felmérések korlátain, és alkalmas a városi WLAN-környezet szerkezeti és biztonsági jellemzőinek trendalapú elemzésére.

A módszertan egyik legfontosabb eredménye, hogy a mérési eljárás kizárólag nyilvánosan sugárzott hálózati jellemzőkre épül, így jogi és etikai szempontból is fenntartható, miközben műszaki értelemben elegendő információt szolgáltat a városi WLAN-végpontok eloszlásának és konfigurációs érettségének jellemzéséhez. Az egységes mérési útvonal, a 2012 óta évente azonos időszakban végrehajtott adatgyűjtés, valamint az idősoros normalizáció együttesen biztosították, hogy a megfigyelt változások elsősorban technológiai és üzemeltetési folyamatokra, ne pedig mérési torzításokra legyenek visszavezethetők.

A külső adatforrásokkal – különösen a WIGLE nyilvános adatbázisával, valamint a Központi Statisztikai Hivatal Budapest lakosságára vonatkozó idősoros adataival – történő összevetés tovább erősítette a módszertan validitását. Az összehasonlító elemzések azt mutatták, hogy a saját mérések által kirajzolt trendek nem elszigetelt jelenségek, hanem a városi környezetben zajló szélesebb technológiai és társadalmi folyamatokkal párhuzamosan jelennek meg.

Az első tézis eredményei egyértelműen megteremtették azt a módszertani alapot, amelyre a további elemzések épülhetnek. E módszertani keret közvetlenül vezet át a következő tézishez, amely már nem az adatgyűjtés és az adatbázis kialakításának kérdésére koncentrál, hanem arra, hogy az így létrehozott idősoros adatok milyen biztonsági mintázatokat és kitettségeket tárnak fel a városi WLAN-környezetben. A második tézisben bemutatom, hogy a végpontok számának növekedése és a technológiai fejlődés ellenére milyen módon maradnak fenn tartósan bizonyos biztonsági kockázatok, és ezek miként azonosíthatók időbeli és térbeli elemzések segítségével.

2.2 A városi WLAN-végpontok biztonsági paramétereinek idősoros és térbeli elemzése

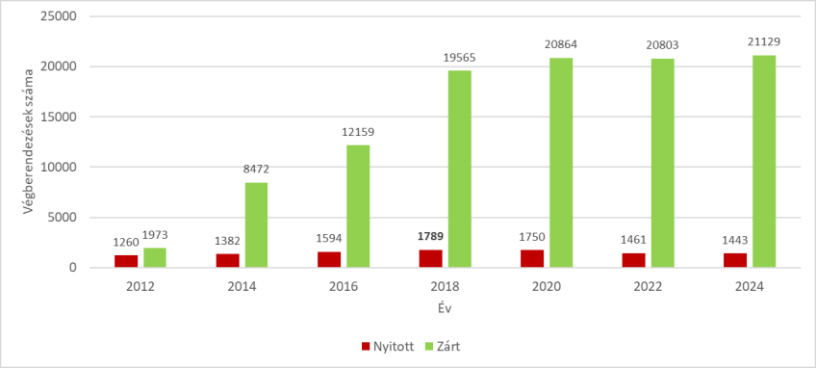
Tézis 2: Igazoltam, hogy az ütemezett wardriving mérések során rögzített vezeték nélküli lokális hálózati végpontok biztonsági jellemzői időben nem homogén módon változnak: a végpontok számának növekedésével párhuzamosan az elavult vagy gyengén védett konfigurációk tartósan jelen maradnak, ami a városi WLAN-környezetben mérhető biztonsági kitettséget eredményez. Ezt a kitettséget a mérési adatok térbeli vizualizációjával validált módon lokalizálni lehet, különös tekintettel a jogosulatlan hozzáférési pontok és interferenciával terhelt környezetek azonosítására. [V2, V3, V7]

Biztonsági jellemzők értelmezése passzív mérések alapján

A vezeték nélküli lokális hálózatok biztonsági állapotának értékelése hagyományosan aktív vizsgálati módszerekhez kötődik, mint például hitelesítési eljárások tesztelése vagy forgalomelemzés. Ezek az eljárások azonban városi léptékben nem alkalmazhatók, sem jogi, sem etikai, sem műszaki okokból [1]. Kutatásaim során ezért a biztonság fogalmát konfigurációs

és üzemeltetési jellemzők mentén értelmeztem, amelyek passzív módon is megbízhatóan rögzíthetők.

A wardriving mérések során gyűjtött adatok közül kiemelt szerepet kaptak az alkalmazott titkosítási és autentikációs mechanizmusok. Ezek a paraméterek közvetlen információt hordoznak a WLAN-végpontok alapvető védelmi szintjéről, különösen akkor, ha nagy elemszámú mintán, idősoros bontásban kerülnek elemzésre [3]. A nyílt hálózatok, az elavult megoldások, valamint a korszerűbb biztonsági mechanizmusok arányának változása jól jellemzi a városi WLAN-környezet biztonsági érettségét. A következő ábra a 2012 és 2024 közötti mérések alapján készült és a nyílt és zárt hálózatok darabszámának alakulását szemlélteti.



6. ábra: Vizsgálati eredmények a zártság szempontjából

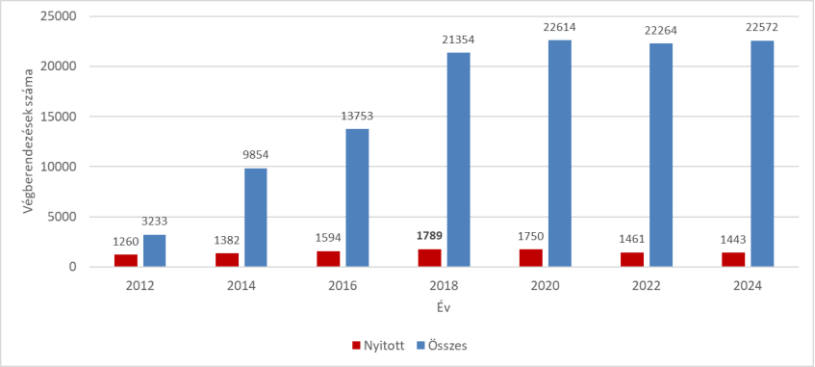
Az idősoros elemzések azt mutatták, hogy a végpontok számának növekedésével nem tűnnek el automatikusan az elavult vagy gyengén védett konfigurációk. Bár az újabb technológiák megjelenése egyértelműen javítja az átlagos biztonsági szintet, a régebbi beállítások tartósan jelen maradnak a városi környezetben. Ez a jelenség arra utal, hogy a technológiai fejlődés önmagában nem garantálja a biztonsági kockázatok megszűnését.

Időbeli nem-homogenitás és biztonsági kitettség

A hosszú idősoros adatbázis lehetővé tette annak vizsgálatát, hogy a biztonsági jellemzők változása milyen mintázatot mutat időben. Az elemzések során egyértelművé vált, hogy a WLAN-környezet biztonsági fejlődése nem lineáris és nem homogén. Egyes időszakokban gyors javulás figyelhető meg, például új szabványgenerációk vagy szolgáltatói beavatkozások megjelenésekor, míg más időszakokban stagnálás vagy lassú változás jellemzi a konfigurációkat.

Ez az időbeli nem-homogenitás különösen jól megfigyelhető akkor, ha a végpontok számát és a gyengén védett hálózatok arányát együtt vizsgáljuk. A mérések azt mutatták, hogy a

végpontok abszolút számának növekedése nem jár együtt a gyengén védett konfigurációk arányának arányos csökkenésével [1]. Ezt szemlélteti a következő ábra.



7. ábra: Végpontszám és gyengén védett hálózatok idősoros ábrázolása

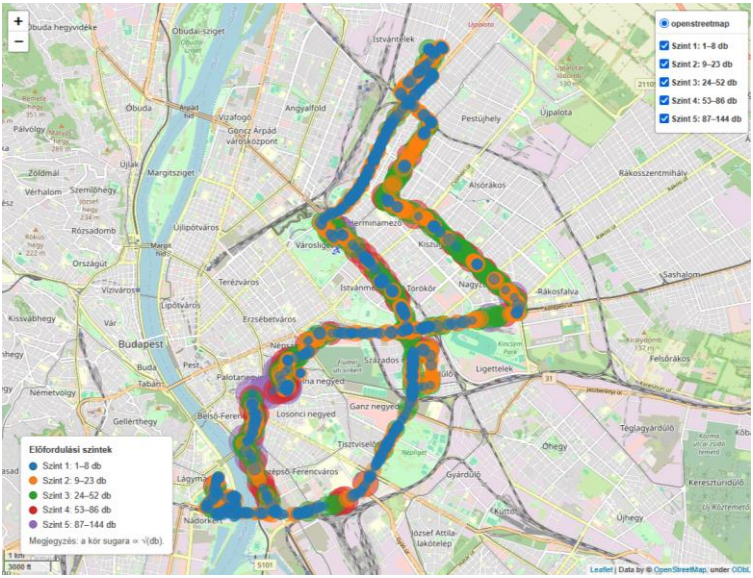
Fontos hangsúlyozni, hogy a „biztonsági kitettség” fogalma ebben a kontextusban nem egyedi hálózatok sebezhetőségét jelenti, hanem a városi környezetben jelen lévő konfigurációk aggregált kockázati potenciálját. A tartósan jelen lévő gyengén védett végpontok növelik a lehetőségét a jogosulatlan hozzáférésnek és az információszivárgásnak.

Térbeli lokalizáció és vizualizáció szerepe

A biztonsági kitettség nemcsak időben, hanem térben is értelmezhető. A wardriving mérésekhez kapcsolódó GPS-

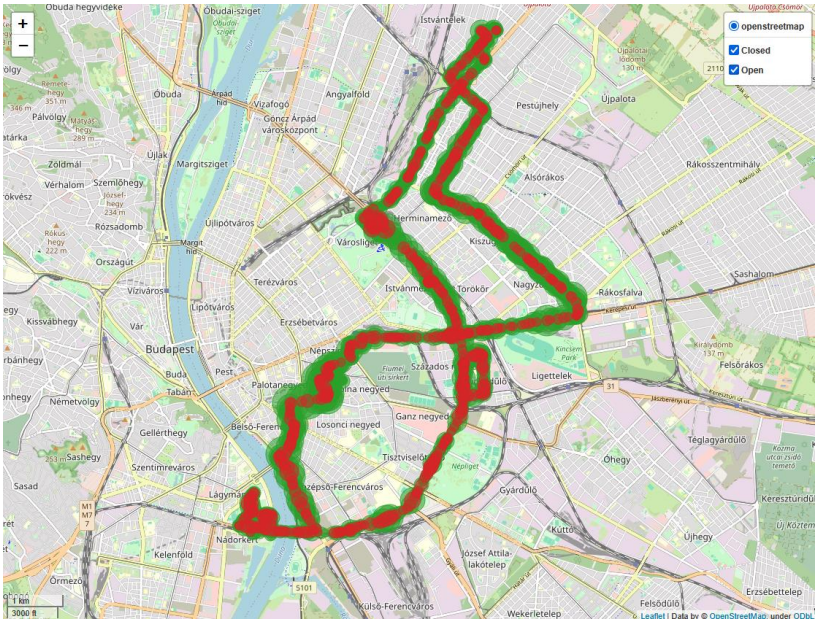
adatok lehetővé tették a WLAN-végpontok térbeli eloszlásának vizsgálatát, valamint a biztonsági anomáliák lokalizálását [9]. A mérési adatok térbeli vizualizációja nem pusztán illusztratív célokat szolgált, hanem elemzési eszközként is funkcionált.

A hőtérképes megjelenítések révén azonosíthatók voltak azok a területek, ahol a gyengén védett vagy szabálytalan konfigurációk sűrűbben fordultak elő. Ezek a területek gyakran egybeestek nagy végpontsűrűségű városi zónákkal, például lakótelepi vagy vegyes funkciójú környezetekkel. Ezt szemlélteti a következő ábra.



8. ábra: WLAN-végpontok megjelenítése végpontsűrűség szerint

A térbeli vizualizáció különösen hasznosnak bizonyult a jogosulatlan hozzáférési pontok beazonosításában. Az ilyen anomáliák nem mindig mutathatók ki pusztán statisztikai elemzéssel, azonban térben megjelenítve jól elkülönülő mintázatokat rajzolnak ki. Ez igazolja, hogy a vizualizáció nem önálló cél, hanem a biztonsági kitettség validált lokalizációjának eszköze. Ezt szemlélteti a következő ábra.



9. ábra: WLAN-végpontok megjelenítése zártság szempontjából

A vizuális megjelenítés lehetővé teszi a zárt (zöld) és a nyitott (piros) WLAN-végpontok egyértelmű elkülönítését, ezáltal

támogatja a városi WLAN-környezet biztonsági kitettségének térbeli értelmezését.

Részösszegzés

A második tézisben bemutatott eredmények alapján megállapítható, hogy a városi vezeték nélküli lokális hálózatok biztonsági állapota nem értelmezhető kizárólag technológiai fejlődési folyamatként. Az ütemezett wardriving mérésekből létrehozott hosszú idősoros adatbázis egyértelműen rámutatott arra, hogy a WLAN-végpontok számának növekedése és a korszerűbb szabványok elterjedése ellenére a gyengén védett vagy elavult konfigurációk tartósan jelen maradnak a vizsgált környezetben. Ez a jelenség a városi WLAN-környezet strukturális biztonsági kitettségére utal, amely nem szűnik meg automatikusan a technológiai megújulással.

Az idősoros elemzések kimutatták, hogy a biztonsági jellemzők változása időben nem homogén: egyes időszakokban gyors javulás figyelhető meg, míg más időszakokban stagnálás vagy csak mérsékelt változás tapasztalható. A végpontok abszolút számának növekedése nem jár együtt a gyengén védett konfigurációk arányos visszaszorulásával, ami azt jelzi, hogy a

városi WLAN-környezet biztonsági szintje heterogén módon fejlődik, és egyes kockázati elemek hosszú távon is fennmaradnak.

A térbeli vizualizációval kiegészített elemzések tovább erősítették ezt a megállapítást. A mérési adatok hőtérképes megjelenítése lehetővé tette a biztonsági anomáliák lokalizálását, és rávilágított arra, hogy a gyengén védett konfigurációk gyakran jól körülhatárolható városi zónákhoz köthetők. A vizualizáció ebben az értelemben nem pusztán szemléltető eszközként jelent meg, hanem a biztonsági kitettség térbeli értelmezésének és validálásának fontos elemévé vált.

A második tézis eredményei összességében azt mutatják, hogy a városi WLAN-környezet biztonsági állapota nem egységesen javuló, hanem több, egymással párhuzamosan létező konfigurációs és üzemeltetési gyakorlat eredőjeként alakul. Ez a megfigyelés közvetlenül felveti annak kérdését, hogy mely tényezők képesek ténylegesen és mérhető módon javítani a vezeték nélküli lokális hálózatok biztonsági jellemzőit városi léptékben.

E kérdés megválaszolásához a következő tézis már nem pusztán leíró és elemző megközelítést alkalmaz, hanem egy konkrét technológiai és üzemeltetési tényező hatását vizsgálja. A

harmadik tézisben bemutatom, hogy a vezetékes szolgáltatást nyújtó szolgáltatók által telepített, integrált WLAN-funkcióval rendelkező végberendezések elterjedése miként járult hozzá a WLAN-végpontok biztonsági jellemzőinek mérhető javulásához a városi környezetben végzett idősoros mérések alapján.

2.3 Szolgáltatói integrált WLAN-funkcióval rendelkező végberendezések elterjedésének biztonsági hatásai városi környezetben

Tézis 3: Igazoltam, hogy a vezetékes szolgáltatást nyújtó szolgáltatók által telepített, integrált WLAN-funkcióval rendelkező végberendezések elterjedése mérhetően javította a vezeték nélküli lokális hálózati végpontok technikai biztonsági jellemzőit, különösen az egységesebb titkosítási és autentikációs konfigurációk megjelenésén keresztül, a városi WLAN-környezetben végzett idősoros mérések alapján. [V1, V5, V6, V8]

A szolgáltatói végberendezések megjelenésének technológiai háttere

A városi WLAN-környezet szerkezetének átalakulásában meghatározó szerepet játszott az a folyamat, amelynek során a vezetékes internetszolgáltatást nyújtó szolgáltatók egyre nagyobb arányban kezdtek integrált WLAN-funkcióval rendelkező végberendezéseket telepíteni az előfizetői oldalon [5]. Ezek az eszközök a vezetékes hozzáférési technológiát és a

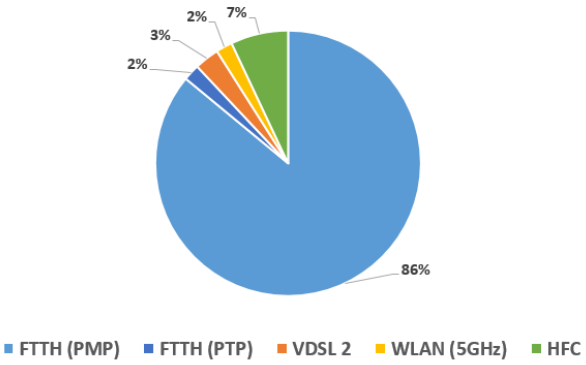
vezeték nélküli hozzáférést egyetlen, előre konfigurált egységben valósítják meg.

Ez a megközelítés alapvetően eltér a korábbi gyakorlattól, amikor a szolgáltató kizárólag a vezetékes végpontot biztosította, míg a WLAN-infrastruktúra kialakítása és üzemeltetése teljes mértékben a felhasználóra hárult. A felhasználói oldalon telepített, önálló hozzáférési pontok konfigurációja gyakran esetleges volt, és jelentős heterogenitást mutatott mind technológiai, mind biztonsági szempontból. A szolgáltatói integrált végberendezések megjelenésével ez a heterogenitás mérhető módon csökkent.

Ez az időszak - 2014-től napjainkig - nem csupán új szolgáltatói eszközök megjelenését jelentette, hanem a szolgáltatói stratégia paradigmaváltását is: a fókusz a puszta elérhető maximális adatátviteli sebességről a felhasználói élményre és a WLAN lefedettség minőségére és biztonságára helyeződött át.

2018 fordulópont volt a hazai vezetékes távközlési piac számára. A SZIP – Szupergyors Internet Program – keretében az ország minden lakosa számára vezetéken vagy egyes helyeken vezeték nélkül legalább 30Mbit/s sebességű internet-szolgáltatást kell biztosítania a szolgáltatóknak. A szolgáltatói infrastruktúra fejlesztése elsősorban optikai megoldásokkal valósult meg. A

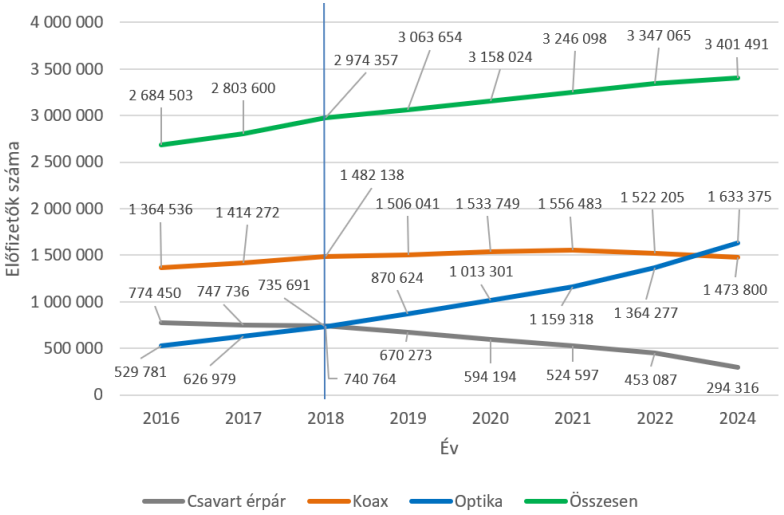
hálózatok bizonyos részein pedig vegyes, úgynevezett Hybrid Fiber-Coaxial (HFC) megoldások kerültek kivitelezésre. Ezekkel a megoldásokkal a már fent említett szolgáltatói végpontok mellett új eszközök is a felhasználókhoz kerültek vezeték nélküli hálózati megoldás támogatással. Az NMHH adatai alapján a SZIP keretében megvalósított technológiák közül a tisztán optikai Fiber to the Home (FTTH) és HFC megoldások voltak a legelterjedtebbek. Ezt mutatja a következő diagramm.



10. ábra: SZIP fejlesztések technológiai megoszlása

Az FTTH esetén optikai végpontot kapott a felhasználó egy szolgáltatói integrált végberendezéssel, míg HFC esetén a felhasználó számára egy koaxiális megoldást támogató hasonló végberendezés került telepítésre. A következő ábra a 2016 és

2024 közötti KSH adatokat szemlélteti a vezetékes internet előfizetések számának és a fizikai közeg szempontjából.



11. ábra: SZIP fejlesztések technológiai megoszlása

Az ábrán jól látszik, hogy 2018 után a SZIP projekt keretében a csavart érpáros végpont bekötések száma folyamatosan csökkent, a koaxiális-optikai és tisztán optikai megoldások száma pedig nőtt.

Biztonsági konfigurációk homogenizációja

A szolgáltatói integrált végberendezések egyik legfontosabb hatása a WLAN-környezet biztonsági konfigurációinak homogenizációja volt. Az idősoros wardriving mérések alapján jól elkülöníthető időszak figyelhető meg, amikor az alkalmazott titkosítási és autentikációs mechanizmusok megoszlása jelentős változáson ment keresztül. A korábban gyakran előforduló nyílt vagy elavult konfigurációk aránya csökkenni kezdett, miközben a biztonságos megoldások váltak dominánssá.

Ez a változás nem magyarázható pusztán a technológiai fejlődéssel vagy az új szabványok megjelenésével, mivel a mérési adatok alapján a végpontok jelentős része továbbra is régebbi hardverplatformokra épült. A döntő különbséget az jelentette, hogy a szolgáltatói eszközök előre definiált, központilag karbantartott konfigurációval kerültek telepítésre. Egy ilyen általános beállítási konfiguráció elemeit szemlélteti a következő ábra.

	A	D	F	G	H	I	J	K	L	M
1	SSID	RSSI	Chan	Width	802.11	Max Rate	Retries	WEP	WPA	WPA2
4794	Telekom-058a4d	-85	100+104+108+112	80	a, n, ac	1733.4	N/A			PSK-CCMP
4795	Telekom-059b5d	-85	100+104+108+112	80	a, n, ac	1733.4	N/A			PSK-CCMP
4796	Telekom-059d88	-79	36+40+44+48	80	a, n, ac	1300.05	N/A			PSK-CCMP
4797	Telekom-059f10	-84	36+40+44+48	80	a, n, ac	1300.05	N/A			PSK-CCMP
4798	Telekom-05a401	-84	100+104+108+112	80	a, n, ac	1733.4	N/A			PSK-CCMP
4799	Telekom-05ad90	-87	36+40+44+48	80	a, n, ac	1300.05	N/A			PSK-CCMP
4800	Telekom-05b940	-90	52+56+60+64	80	a, n, ac	1733.4	N/A			PSK-CCMP
4801	Telekom-05b9cc	-88	100+104+108+112	80	a, n, ac	1733.4	N/A			PSK-CCMP
4802	Telekom-05bea3	-91	52+56+60+64	80	a, n, ac	1733.4	N/A			PSK-CCMP
4803	Telekom-05c47d	-84	100+104+108+112	80	a, n, ac	1733.4	N/A			PSK-CCMP
4804	Telekom-05c9af	-83	52+56+60+64	80	a, n, ac	1733.4	N/A			PSK-CCMP
4805	Telekom-05d408	-89	100+104+108+112	80	a, n, ac	1300.05	N/A			PSK-CCMP
4806	Telekom-05fb40	-87	104	20	a, n, ac	1300.05	N/A			PSK-CCMP
4807	Telekom-062338	-78	36+40+44+48	80	a, n, ac	1300.05	N/A			PSK-CCMP
4808	Telekom-0871c4	-89	100+104+108+112	80	a, n, ac	1733.4	N/A			PSK-CCMP
4809	Telekom-088bfd	-91	100+104+108+112	80	a, n, ac	1733.4	N/A			PSK-CCMP

12. ábra: Szolgáltatói végberendezések rögzített paraméterei

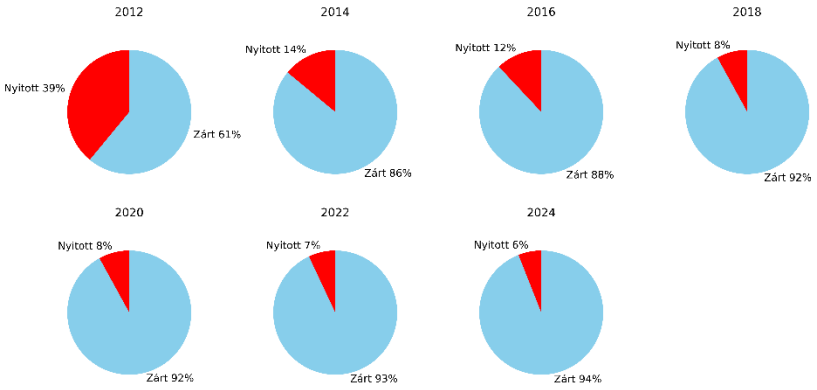
A szolgáltatói végberendezések olyan „alapértelmezett biztonsági szintet” valósítanak meg, amely ugyan nem tekinthető optimálisnak minden esetben, de jelentősen javítja az átlagos biztonsági állapotot. Ez azért fontos, mert a felhasználói oldalra bízott konfigurációs döntések gyakran vezetnek alulkonfigurált WLAN-hálózatokhoz.

A harmadik tézis alátámasztásának kulcsa az idősoros mérési adatok elemzése volt. A mérések lehetővé tették annak vizsgálatát, hogy a szolgáltatói integrált végberendezések megjelenése nem eseti jelenség, hanem hosszabb távú, mérhető hatást gyakorol a városi WLAN-környezetre.

Az elemzések során a titkosítási mechanizmusok megoszlását nem abszolút értékekben, hanem relatív arányokban vizsgáltam, figyelembe véve a végpontszám folyamatos növekedését. Az így

kapott idősorok jól mutatták, hogy a szolgáltatói eszközök elterjedésével párhuzamosan csökkent a technológiailag gyengén védett konfigurációk aránya, miközben nőttek az egységes, korszerűbb megoldások.

Szeretném leszögezni, hogy a tézis nem állít kizárólagos oksági kapcsolatot. A mérési adatok alapján azonban egyértelmű összefüggés figyelhető meg a szolgáltatói integrált végberendezések elterjedése és a WLAN-végpontok biztonsági jellemzőinek javulása között, amely empirikusan igazolható. Ezt szemlélteti a következő ábra, amely százalékos arányban mutatja a nyitott és zárt hálózatok alakulását.



13. ábra: Vizsgálati eredmények a zártság szempontjából százalékos arányban

2018 után megfigyelhető, hogy a zárt és nyitott hálózati végpontok aránya nagyon lassú ütemben változik.

Részösszegzés

A harmadik tézisben bemutatott eredmények alapján megállapítható, hogy a városi WLAN-környezet biztonsági állapotának alakulásában nem kizárólag a vezeték nélküli technológiák fejlődése játszik szerepet, hanem meghatározó hatással bírnak az üzemeltetési és telepítési gyakorlatok is. A vezetékes szolgáltatást nyújtó szolgáltatók által telepített, integrált WLAN-funkcióval rendelkező végberendezések elterjedése olyan strukturális változást idézett elő, amely mérhető módon javította a vezeték nélküli lokális hálózati végpontok biztonsági jellemzőit a vizsgált városi környezetben [5].

Az idősoros wardriving mérések alapján kimutatható volt, hogy a szolgáltatói eszközök megjelenésével párhuzamosan csökkent a technológiailag elavult, vagy gyengén védett konfigurációk aránya, miközben nőtt az egységesebb, korszerűbb titkosítási és autentikációs megoldások alkalmazása. Ez a változás nem tekinthető pusztán technológiai determinációnak, mivel az

azonos időszakban továbbra is jelen voltak olyan végpontok, amelyek nem részesültek szolgáltatói konfigurációs kontrollban. A megfigyelt javulás ezért elsősorban az integrált végberendezések által biztosított alapértelmezett beállítások és a központosított üzemeltetés hatásának tulajdonítható.

3 A kutatás és a bemutatott eredmények hatása, visszhangja

A kutatásaimat és azok eredményeit folyóiratcikkekben és könyvfejezetekben, valamint hazai és nemzetközi tudományos konferenciákon publikáltam és mutattam be. A mai napig - 2026.02.10. - összesen 87 közleményem szerepel a Magyar Tudományos Művek Tárában, amelyek közül 70 közlemény a PhD-fokozat megszerzését - 2013 - követően jelent meg. Az általam jegyzett vagy társszerzőként publikált közleményekre 145 független hivatkozás érkezett, ezek közül 59 Web of Science és 32 Scopus adatbázisban indexált. Hirsch-indexem 7. A kutatásaim eredményei az oktatásban is hasznosultak, magyar nyelvű tananyagok fejlesztésén keresztül. A következő tudománymetriai összefoglaló táblázat a Tud-O-Méter MTMT-ből vett adatai alapján készült.

	Pontszám
Q szám összesen:	7.256
Q szám cikkekből:	7.156
Q szám könyvből:	0.100
I szám:	145
I szám WoS idézetekből:	59
Impakt faktor:	8.100
Relatív impakt faktor:	2.083

	Pontszám
IF-es cikkek száma:	5
Egyszerzős IF-es cikkek:	0
H index:	7
Összes idéző:	166
Összes publikáció:	87

4 Irodalmi hivatkozások listája

[1] Zs. Haig and L. Kovács, *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest, Magyarország: Nemzeti Közszolgálati Egyetem, 2012. [Online]. Elérhető: https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf

[2] Cisco Systems, *Annual Internet Report (2018–2023)*, 2023. [Online]. Elérhető: https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

[3] IEEE Standards Association, *IEEE 802.11 Wireless Local Area Networks*, 2025. [Online]. Elérhető: https://www.ieee802.org/11/

[4] Kormányzati Informatikai Fejlesztési Ügynökség, *Szupergyors Internet Program (SZIP),* [Online]. Elérhető: https://kifu.gov.hu/projekt/szupergyors-internet-program-szip/

[5] Grandmetric, *Wi-Fi Standards Evolution*, [Online]. Elérhető: https://www.grandmetric.com/wi-fi-standards-evolution/

[6] Központi Statisztikai Hivatal, *Helyhez kötött internet előfizetések száma hozzáférési szolgáltatások szerint*, 2024. [Online]. Elérhető: https://www.ksh.hu/stadat_files/ikt/hu/ikt0025.html

[7] Nemzeti Média- és Hírközlési Hatóság, *A helyhez kötött elektronikus hírközlési piac helyzete*, 2024. [Online]. Elérhető: https://nmhh.hu/dokumentum/249667/helyhez_kotott_piaci_jelentes_2020_harmadik_2024_masodik_negyedev.pdf

[8] Duckware, *Wi-Fi 4/5/6/6E (802.11n/ac/ax)*, szept. 3, 2022. [Online]. Elérhető: https://www.duckware.com/tech/wifi-in-the-us.html

[9] Wireless Geographic Logging Engine (WiGLE), WiGLE.net, [Online]. Elérhető: https://wigle.net

[10] S. Lindroos, A. Hakkala, and S. Virtanen, "A systematic methodology for continuous WLAN abundance and security analysis," Computer Networks, vol. 197, art. no. 108359, 2021. doi: 10.1016/j.comnet.2021.108359

5 A tézispontokhoz kapcsolódó tudományos közlemények

[V1] Varga, Péter János, Wardriving to analyse the societal impact of wireless networks – an engineering perspective, In: IEEE - Óbudai Egyetem; IEEE (szerk.) 2023 IEEE 6th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE) : Proceedings Danvers (MA), Amerikai Egyesült Államok : Institute of Electrical and Electronics Engineers (IEEE) (2023) 371 p. pp. 143-147. , 5 p.

[V2] Zsolt, Illési ; Áron, Halász ; Péter, János Varga, Wireless Networks and Critical Information Infrastructure, In: Szakál, Anikó (szerk.) IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI 2018), Temesvár, Románia : IEEE Romania Section, IEEE Hungary Section (2018) 604 p. pp. 255-260. , 6 p.

[V3] Kornél, Gyöngyösi ; Péter, János Varga ; Zsolt, Illési WLAN heat mapping in hybrid network, In: Valerie, Novitzká; Štefan, Korecko; Anikó, Szakál (szerk.) INFORMATICS 2017, 2017 IEEE 14th International Scientific Conference on

Informatics Proceedings, Kosice, Szlovákia : IEEE Hungary Section (2017) 437 p. pp. 94-97. , 4 p.

[V4] Varga, Péter János, A vezeték nélküli hálózatok fejlődése és hatásai a digitális társadalom formálásában, In: Wührl, Tibor (szerk.) KVK Habilitációs és PhD Workshop Minikonferencia : Kiadvány kötet, Budapest, Magyarország : Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar (2024) 124 p. pp. 13-20. , 8 p.

[V5] Varga, Péter János ; Illési, Zsolt, Wi-Fi 6 Application in Iot Environment, INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 20 : 3 pp. 277-283. , 7 p. (2022)

[V6] Varga, Péter János, Vezeték nélküli hálózatok társadalomra gyakorolt hatása mérnöki szempontból, In: Molnár, György; Wührl, Tibor (szerk.) KVK Habilitációs Workshop Minikonferencia, Budapest, Magyarország : Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar (2023) 93 p. pp. 86-93. , 8 p.

[V7] Haig, Zsolt; Illési, Zsolt; Varga, Péter János, Possibilities of Electronic Jamming of WLAN Networks in the Physical Layer, HADMÉRNÖK 17 : 3 pp. 133-152. , 20 p. (2022)

[V8] Varga, Péter János, Az okos otthonok vezeték nélküli alkotóelemeinek biztonsága, KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 9 : 1-2(21-22) pp. 83-87. , 5 p. (2017)

6 További tudományos közlemények

MTMT-ben az alábbi linken található a teljes publikációs lista:

https://m2.mtmt.hu/gui2/?type=authors&mode=browse&sel=10033565&view=simpleList