

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

IoT Rendszerek Sérülékenység Vizsgálatának Kutatása

Jelige: *Dragon IoT*

Pályamunka lezárásának időpontja: 2023.11.

2025.

Tartalomjegyzék

1.	Bevezetés	3
2.	Internet of Things megvalósulása	4
2.1.	M2M és IoT, IIoT összehasonlítása	5
2.2.	Az IoT technológiák csoportosíthatósága.....	6
2.2.1.	IoT technológiák csoportosítása kiterjedés szerint	6
2.2.2.	Kis hatótávolságú technológiák részletes ismertetése.	9
3.	Biztonsági és Sérülékenységi kérdések az IoT-ben	11
4.	Frekvenciatartományban alkalmazható zavarási módok	12
4.1.	Spot zavarás a sávtartomány elején, közepén és végén.....	12
4.2.	Sweep zavarás a teljes sávtartományban	12
4.3.	Teljes sávtartomány zavarása	12
5.	Zavarás megvalósítása SDR berendezéssel.....	13
5.1.	Zavar vizsgálatok megtervezése, kialakítása	16
5.2.	Zavar vizsgálatok tesztelése	19
6.	Továbbfejlesztési lehetőségek.....	24
7.	Összefoglaló.....	25
8.	Rövidítésjegyzék	26
9.	Irodalomjegyzék	28
9.1.	Források	28
9.2.	Ábrák	31
9.3.	Táblázatok	31

1. Bevezetés

Napjainkban az IoT (Internet of Things), mint kifejezés egyre több helyen jelenik meg és kijelenthetjük, hogy a technológia forradalmát éljük. Több gyártó és szolgáltató használja a fogalmat mind általános, mind ipari területeken. Így fontosnak tartom a tématerület feldolgozását és bemutatását a civil emberek számára, akik nem jártasok a technológiában. Különös tekintettel arra, hogy milyen rendszereket alakíthatnak ki a megvásárolható eszközökkel, mint például okos órák, okos telefonok, különböző szenzorok (hőmérséklet, páratartalom stb.).

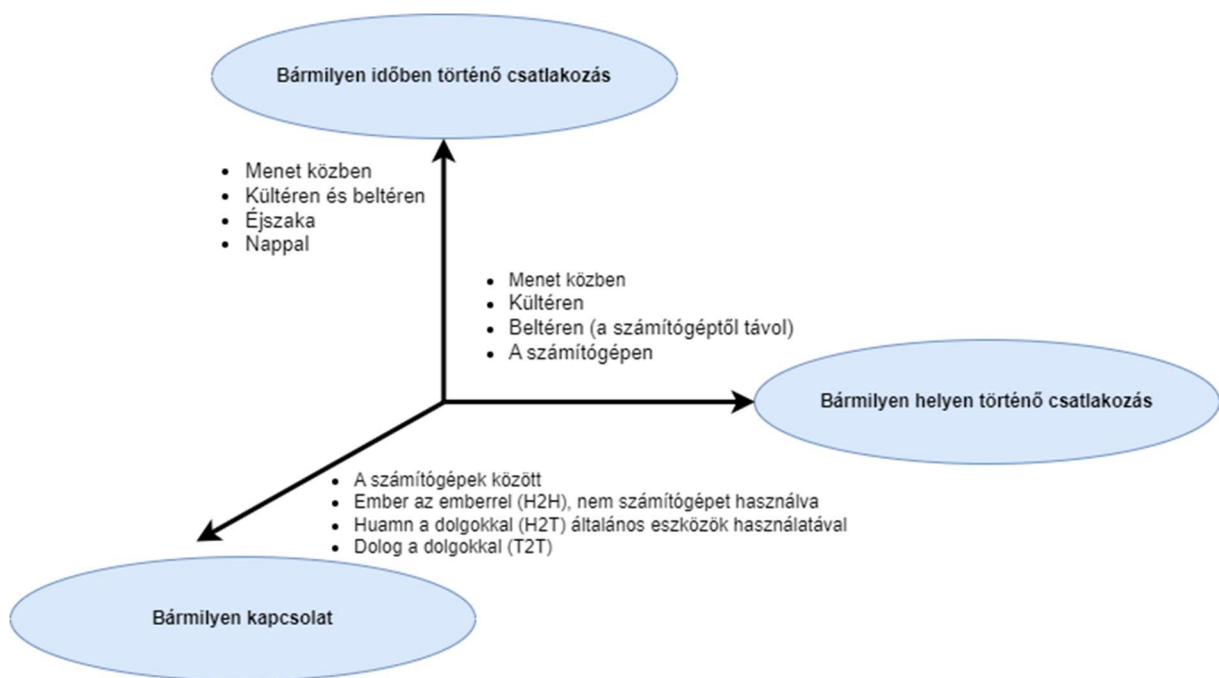
Munkámban az IoT rendszerek sérülékenység vizsgálatára térek ki, de fontosnak tartom bemutatni az Internet of Things fogalmát és alapvető célkitűzéseit is, összehasonlítva az M2M (Machine to Machine) és az IIoT (Industrial Internet of Things) technológiákkal. A továbbiakban bemutatom a fogalmak csoportosíthatóságát többek között kiterjedés szerint és az IoT-ben használt technológiákat, mint például a Bluetooth, Wi-Fi, Zigbee és a Matter-t. Az IoT rendszerek sérülékenysége egy fontos pont a felhasználás terén. Egy rövid betekintést fogok nyújtani az IoT biztonságtechnikai kérdéseibe, többek között a frekvencia tartományban rejlő sérülékenységekre. Ábrákkal szemléltetem az egyes zavarási módokat, mint a teljes sáv zavarása, a vizsgált frekvencia tartomány elején, közepén és végén történő zavarás és a tartományon áthaladó sweep zavarás.

Végezetül pedig az általam összeállított mérési környezetek kerülnek bemutatásra, amelyeken a frekvenciatartományban történő zavarási típusokat fogom vizsgálni és értékelni. A munkámat a jövőben ki szeretném egészíteni a zavarások teljeskörű fizikai megvalósításával és részletes dokumentálásával, valamint fel fogom térképezni a további sérülékenységeket a technológiával kapcsolatban.

2. Internet of Things megvalósulása

Az Internet of Things rövidítve IoT napjainkban rohamosan fejlődik, ezáltal több és több felhasználót képes elérni. A hazai szakirodalomban a „dolgok internete” formájában találkozhatunk a témával kapcsolatos publikációkkal előadásokkal.

Az IoT mint kifejezés, fogalom 1999-ben jelent meg abból a célból, hogy a logisztikai információáramlás gyorsabbá váljon. A kiinduló ötlet alapja az RFID (Radio Frequency IDentification) technológia. Ha a termékeket, árukat ellátjuk RFID jelölővel, akkor az egyes állomásokon egyszerűen beolvasásra kerül a jelölő és rögtön bejegyzés kerülhet a logisztikai rendszerbe az aktuális állapotról például: „előkészítés a szállításra”. 2004 augusztusában az ITU közzétett egy ábrát „Opportunities and Strategic Issues” címmel, amely szemlélteti az IoT kezdeti elgondolását, lényegét. Az elgondolást az első ábra szemlélteti.



1. ábra: IoT technológia kezdeti elképzelése

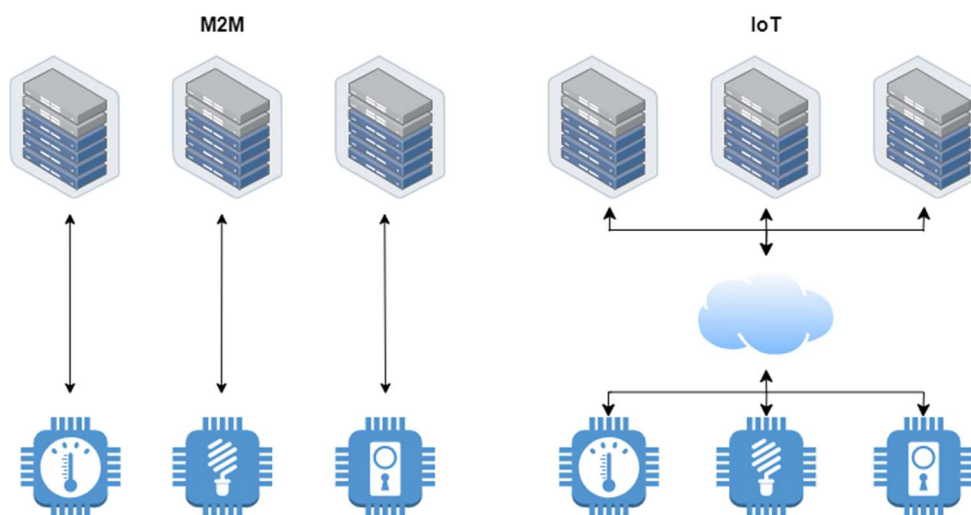
Forrás: Saját szerkesztés, <https://cutt.ly/ywQZ9pAh> alapján

Az ábrán látható a technológia három alappillére, hogy bármilyen időben, bármilyen helyen és bármilyen kapcsolat megvalósuljon. Nem sokkal később, 2005-ben az ITU kiadott egy beszámolót „The Internet of Things” címmel, amelyben részletesen kitértek a jövőbeli víziókra, megvizsgálták az alap technológiákat és a piaci lehetőségeket, valamint a kihívásokat és a tágabb értelemben vett következményeket, illetve a technológia által biztosított előnyök egy részét.

Az Internet of Things fogalom a 2010-es évektől terjedt el világszerte. 2011-ben a feltörekvő technológiák közé is felvették. 2014-ben a Google is elismerte az IoT fontosságát leginkább a szenzorok iránti viszonylatban. Napjainkban eljutottunk odáig, hogy a „dolgok internetéhez” csatlakoztatott eszközök száma meghaladja a 15 milliárdos határt. Hazánkban a legismertebb IoT megvalósítási koncepció az Okos város (Smart city) projektek. [1], [2]

2.1. M2M és IoT, IIoT összehasonlítása

Az IoT technológia előtt már ismert volt az M2M (Machine to Machine), azaz eszköz az eszközzel történő kommunikáció, amely az alapját képezi az IoT-nek. Az M2M kommunikáció két vagy akár több gépet is összeköthet és biztosítja számunkra, hogy emberi beavatkozás nélkül kommunikálhassanak egymással és adatcserét végezzenek. Míg ezzel szemben az IoT olyan eszközök hálózatát alakítja ki, amely érzékelőkkel, szenzorokkal és szoftverekkel rendelkezik, hogy az interneten keresztül kapcsolatot teremtsenek és adatokat továbbítsanak.



2. ábra: M2M és IoT strukturális összehasonlítása

Forrás: Saját szerkesztés

Összességében azt tudjuk elmondani a két technológiáról, hogy megoldást biztosítanak az adatok tárolására, gyűjtésére és eszközök közötti cseréjére, nagyon csekély emberi beavatkozás mellett.

Fontos megemlíteni az ipari alkalmazhatóságát az IoT-nek, amely az IIoT (Industrial Internet of Things) nevet kapta, mint a „dolgok ipari internete”. Ez az elnevelés az ipari számítógépekre kapcsolt szenzorokra, műszerekre és egyéb informatikai eszközökre utal, amelyek egy közös hálózatban tudnak kommunikálni a számítógépek ipari alkalmazásaival, akár a gyártást, tesztelést, energiagazdálkodást és a raktározást is beleértve. Így az IIoT technológiával még naprakészebb adatokat tudunk kapni, amelyek felhasználásával folyamatosan javíthatjuk és optimalizálhatjuk a termelékenységet is. [3], [4], [5]

2.2. Az IoT technológiák csoportosíthatósága

Az IoT által használt technológiákat fontos csoportosítanunk, mivel ezek különböző típusú hálózatok, és eltérő műszaki tulajdonságokkal rendelkeznek. A bemutatott jellemzők fontosak lesznek az első számú sérülékenységi vizsgálatban, amely a sávtartományi sérülékenységi vizsgálatot mutatja majd be.

2.2.1. IoT technológiák csoportosítása kiterjedés szerint

Az IoT technológiákat két fő csoportra oszthatjuk áthidalható hatótávolság szerint. Az egyik a nagy kiterjedésű hálózatok (WAN – Wide Area Networks) míg a másik a kis hatótávolságú technológiák, hálózatok (Short Range Technologies).

A nagy kiterjedésű hálózatokat három csoportra tudjuk felosztani:

- Cellás hálózat,
- Kis teljesítményű nagy kiterjedésű hálózatok (LPWAN - Low Power Wide Area Network),
- Műholdas IoT.

A cellás hálózatok közé tartoznak a mobilhálózati technológiák, mint a 2G, 4G és az 5G-s hálózataink. A harmadik generációs hálózatokat már nem sorolom ide, mivel 2020-ban megkezdődött a technológia kivezetése Magyarországról. Erre azért van szükség, hogy a 3G által használt erőforrásokat másik mobiltechnológiában fel lehessen használni. Frekvenciasáv szempontjából a mobilhálózatok mindegyike engedélyköteles sávtartományban üzemel, amelyet Magyarországon az NMHH (Nemzeti Média és Hírközlési Hivatal) kezel és ad ki bérbe az egyes szolgáltatóknak meghatározott időre.

A következő hálózati típus a kis teljesítményű nagy kiterjedésű hálózatok (LPWAN - Low Power Wide Area Network). Ebbe a csoportba tartozik az Nb-IoT (Narrowband IoT), LTE-M (Long Term Evolution for Machines), SigFox és a LoRa technológia. Az Nb-IoT egy „keskeny sávú” speciális hálózat, mely megbízható, olcsó és ezek mellett biztonságos adatátvitelt, biztosít. A technológia használatához egy SIM (Subscriber Identity Module) modulra van szükségünk és egy fejlesztő keretre vagy modulra. Az LTE-M mondhatni ugyan olyan, mint az Nb-IoT viszont a feltöltési és letöltési sebességekben már jobb paramétereket biztosít. Mivel ezekhez a technológiákhoz mobilhálózati kapcsolat szükséges, így frekvenciasáv felhasználása szempontjából engedélyköteles sávhoz tartoznak. A SigFox technológiának a fő célja az IoT eszközök és különféle szenzorok kommunikációjának a biztosítása nagy hatótávolságon keresztül, amely akár 20-30 km-es távolságot is lefedhet. A LoRa technológia mondhatni megegyezik a SigFox-al a legszembetűnőbb különbség az egyes technológiák költségigénye. Az említett két technológia a nem engedélyköteles frekvenciasávba tartozik.

A műholdas IoT hálózati típusnál az NTN-IoT (None-Terrestrial Networks) technológia jelent meg a 3GPP (3rd Generation Partnership Project) realese 15-től, amely lehetővé teszi a nem földfelszíni szolgáltatást. Legnagyobb előnye, hogy kontinenseket vagy akár a teljes földet le tudja fedni. Emellett viszont alacsony az adatátviteli sebességünk, illetve nagy a késleltetés. Ez a technológia frekvenciatartomány szempontjából az engedélyköteles tartományokhoz sorolható.

A kis hatótávolságú hálózatok szintén három csoportra tudjuk felosztani:

- Helyi hálózatok (LAN - Local Area Network),
- Mesh LAN,
- Személyi hálózatok (PAN - Personal Area Network).

A helyi hálózatok közé tartozik a Wi-Fi (Wireless Fidelity), illetve az Ethernet technológia. Amelyek alapvetően biztosítják otthonainkban az IoT eszközök információáramlását. Gondolva itt a hőmérsékletérzékelők, pártartalom szenzor és különböző okos eszközeinkre. Ez a két technológia mondhatni minden háztartásban elérhető.

A Mesh LAN hálózati típusba tartozik napjaink legismertebb technológiái, a Zigbee és a Matter. A Zigbee elgondolása az volt, hogy minden eszközünket, amely körülöttünk megtalálható, egy automatikus rendszeren keresztül lehessen vezérelve egyetlen hálózaton keresztül. A Matter ugyanazon elgondoláson alapul, mint a Zigbee, viszont itt már nem kell a kompatibilitás miatt aggódnunk. Ebben a technológiában minden gyártó eszköze ugyanúgy tud működni, legyen az akár Apple, Amazon vagy Google és más gyártó termékei.

A kis hatótávolságú technológiák közé sorolható még a személyi hálózatok PAN (Personal Area Network), mint például a Bluetooth, RFID és az NFC. A három technológia előnye, hogy kis hatótávolsági paraméterekkel rendelkeznek. A fentiekben említett három hálózattípusban egyik technológia sem engedélyköteles frekvenciasáv szempontjából. Az IoT technológiák csoportosítását az 1. táblázat foglalja össze. [2], [4], [5]

	Hálózat típusa	Frekvenciasáv	Technológia
Nagy kiterjedésű hálózatok (WAN - Wide Area Networks)	Cellás (WAN - Wide Area Network)	Engedélyköteles	GSM - 2G
			4G/5G
			Nb-IoT, LTE-M
	Kis teljesítményű nagy kiterjedésű hálózatok (LPWAN - Low Power Wide Area Network)	Nem engedélyköteles	SigFox
			Lo-Ra
	Műholdas IoT	Engedélyköteles	NTN-IoT (5G)
Kis hatótávolságú technológiák (Short Range Technologies)	Helyi hálózatok (LAN - Local Area Network)	Nem engedélyköteles	Wi-Fi, Ethernet
	Mesh LAN		Zigbee, Matter
	Személyi hálózatok (PAN - Personal Area Network)		Bluetooth, RFID, NFC

1. táblázat: IoT technológiák általános csoportosítása

Forrás: Saját szerkesztés, [2], [4], [5] alapján

2.2.2. Kis hatótávolságú technológiák részletes ismertetése

A kis hatótávolságú technológiák műszaki paramétereinek ismerete fontos a sérülékenységi vizsgálataim szempontjából, így megvizsgálom a technológiák:

- frekvencia spektrumban való elhelyezkedését,
- mely szabványok írják le az egyes technológiákat,
- milyen hálózati struktúrába sorolhatók,
- adatsebességüket,
- hatótávolsági paramétereiket.

Spektrumban való elhelyezkedésük szempontjából a Bluetooth technológiát alkalmazó eszközeink a 2,4 - 2,4835 GHz-es sávban üzemelnek. Ez az ISM (Industrial Scientific and Medical) sáv, amely az ipari, kutatási és egészségügyi eszközök működési tartományának jelöltek ki. A Wi-Fi technológia három frekvenciasávban található meg: 2,4GHz, 5GHz és 6GHz. A 2,4GHz-es Wi-Fi 14 csatornával rendelkezik, amelyek 22MHz-esek viszont csak 3 olyan csatorna van, amelyek nem fedik egymást (1, 6, 11). Az 5GHz-es Wi-Fi-nél 21 darab egymást nem átfedő csatorna található, amelyek 20MHz-esek vagy 9 darab 40MHz-es csatorna valósítható meg. A 6GHz-es Wi-Fi-nél pedig 160MHz-es csatornákat tudunk kialakítani. Az RFID három sávban helyezkedik el 125kHz, 13,56MHz és 868MHz. Az NFC technológia szintén 13,56MHz-en. Fontos megemlíteni a Zigbee-t és a Matter-t, mivel ezek napjainkban a fő technológiák, amelyek biztosítják magát az IoT-t. Ezek a technológiák 2,4GHz-en (Global), 915MHz-en (America) és 868MHz-en (Europe) üzemelnek.

Az egyes technológiákról különböző szabványokból tájékozódhatunk. A vezeték nélküli technológiákat az IEEE 802.15. x-es szabványokban találhatjuk meg, de más szabvány is tárgyalja, mint az ISO, IEC.

Hálózati struktúrák szempontjából a Bluetooth, RFID és az NFC esetében Pont-Pont kapcsolatról beszélhetünk, míg a Wi-Fi esetében WLAN vagy is vezeték nélküli helyi hálózati kapcsolatról. A Zigbee és Matter esetében pedig már az eszközeinkből felépülő különböző hálózati struktúrák valósulhatnak meg, mint a csillag, fa és a mesh topológia.

Adatsebesség viszonylatában a Wi-Fi technológiát mondhatjuk kiemelkedőnek, mivel akár az elméleti 9.6 Gbps-os adatátviteli sebességet is elérhetjük. A Wi-Fi mint technológia folyamatosan fejlődik és egyre jobb adatátviteli sebességet és jobbnál jobb jellemzőket tudunk elérni. Napjainkban az ax-es Wi-Fi routerek a legjobbnak mondhatók, amelyek Wi-Fi 6-os szabványt használ az IEEE 802.11ax-szerint.

A hatótávolság szempontjából az NFC és az RFID rendelkezik a legkisebb értékkel, amelyek 0,1-0,2 méter és 1 méteres távolságban biztosítják a szolgáltatásokat. A Bluetooth megközelítőleg 8-10 méteres területet képes lefedni, ezt minden felhasználó tapasztalhatja saját eszközei révén, mint például hangszórók, fülhallgatók vagy Bluetooth-os egerek és billentyűzetek révén. A Zigbee és Matter esetében 10 - 20 méterről beszélhetünk, amely kevésnek tűnik, de a Wi-Fi hálózatunk kiegészítésével kellő lefedettséget tud biztosítani otthonainkban található IoT eszközeinek. A sorban a Wi-Fi-nek mondható a legnagyobb lefedettsége a kis hatótávolságú technológiák közül, amely típusoktól függően 10 – 140 méteres hatótávolságról beszélhetünk beltéren. A kis hatótávolságú technológiákat a 2. ábra foglalja össze. [2], [4], [5]

Technológia	Bluetooth	Wi-Fi	RFID	NFC	Zigbee, Matter
Spektrum	Nem engedélyköteles frekvenciasáv				
	2,4 GHz - 2,4835 GHz ISM (Industrial, Scientific and Medical)	2,4 GHz 5GHz 6GHz	125 kHz (LF sáv) 13,56 MHz (HF sáv) 868 MHz (UHF sáv)	13,56MHz	2,4GHz (Global) 915MHz (America) 868 MHz (Europe)
Specifikáció/ Szabvány	IEEE 802.15.1	IEEE 802.15.1	Több Szabvány	ISO/IEC 14443 ISO/IEC 18000-3	IEEE 802.15.11 a...
Hálózat struktúra	Pont-Pont	WLAN	Pont-Pont	Pont-Pont	Csillag, Fa, Mesh
Adatsebesség	1 - 24Mbps	0,9-9,6Gbps	423kbps	424kbps	20 - 250kbps
Hatótávolság	8 - 10m	10 - 140m	1m	0,1 -0,2m	10 - 20m

2. táblázat: Kis hatótávolságú technológiák ismertetése

Forrás: Saját szerkesztés, [2], [4], [5] alapján

Vizsgálataimban a Bluetooth és a Wi-Fi technológiák paraméterei lesznek fontosak számomra, mert mérés kialakításaimat ezekhez kell megterveznem.

3. Biztonsági és sérülékenységi kérdések az IoT-ben

Az IoT eszközök, rendszerek folyamatosan bővülnek, a 2030-as évben a becslések szerint a 75-100 milliárdos eszközszámot is elérjük, amely megközelítőleg 10 készüléket jelent emberenként a világon. Így fontos tisztában lenni az eszközök biztonsági és sérülékenységi részeivel. A kiberbűnözők egyre nagyobb számban keresik a lehetőségeket, a rendszerekben megtalálható kiskapukat, hogy közelebb férkőzzenek adatainkhoz és azokon keresztül hozzánk.

Általánosan kijelenthetjük, hogy a lakossági IoT eszközök gyenge vagy semmiféle védelemmel sincsenek ellátva, így az esetleges támadó könnyedén átkonfigurálhatja, és saját eszközeként tudja használni az otthonainkban megtalálható berendezéseinket. Az ilyen támadások legnagyobb hányada abból ered, hogy az alapértelmezett jelszó nem kerül megváltoztatásra vagy nem megfelelő „erősségű” jelszót használunk. Egy erős jelszóban nagy és kisbetűs karakternek, számnak és speciális karakternek is szerepelnie kellene.

A biztonsági kérdés a forgalomirányítóknál (router) és azok konfigurációjánál kezdődik. A forgalomirányítón keresztül távolról is tudunk kommunikálni eszközeinkkel. Ennek tudatában, ha valaki hozzá szeretne férni eszközeinkhez, akkor legnagyobb eséllyel a nem megfelelően beállított forgalomirányítótól fog elindulni. Azonban ha alapvető beállításokat elvégzünk, akkor nagymértékben megnehezíthetjük a támadó dolgát és nem lesz elsődleges célpont a bejutni a mi hálózatunkba.

A fizikai fenyegetettségekre is hangsúlyt kell fektetnünk, legyen szó akár a biztonsági kameráinkról, szenzorainkról és okos eszközeinkről. Ha példaként veszünk egy okos termosztátot, amit már egy hekker figyel és elér, távolról könnyedén megállapíthatja, hogy mikor megyünk el otthonról és mikor érünk haza. Ennek tudatában már akkor tud fizikailag bejutni otthonainkba, amikor senki nem tartózkodik otthon.

Kísérleteim során az eszközök zavarhatóságát fogom vizsgálni frekvenciatartományi szempontból, amelyek a Wi-Fi és Bluetooth technológiát alkalmazó eszközökre terjed ki. A részletes bemutatást a későbbi fejezetben részletesen fogom tárgyalni. [6], [7]

4. Frekvenciatartományban alkalmazható zavarási módok

A frekvenciatartományban való vizsgálatok előtt fel kell térképezni a lehetséges zavarási módokat. A zavarási módok közül a következő három a legelterjedtebb:

- a sávartomány elején, közepén és végén megvalósuló zavarás,
- sweep zavarás a teljes sávartományon keresztül,
- a teljes sávartomány zavarása.

Ebben a fejezetben ezeket a zavarási módokat fogom bemutatni, amelyeket a vizsgálataim alatt alapul fogok használni. Minden zavarási technika előtt meg kell vizsgálni a zavarni kívánt technológia által alkalmazott sáv paramétereit, hogy hol találjuk a sávban és mely értéken helyezkedik el az alsó és felső határfrekvenciája. [8], [9]

4.1. Spot zavarás a sávartomány elején, közepén és végén

Az első lehetséges zavarási mód, amikor a meghatározott sáv elején, közepén és végén fogok zavarni egy általam meghatározott szélességű jellel. A szélességet érdemes a technológia által alkalmazott sávartományi felosztás mintájára alkalmazni. A kialakítás akkor a legsikeresebb, ha a vivő jelet sikerül elnyomnunk, és ez által szakadozni kezd vagy számunkra legkedvezőbb esetben teljesen megszakad a kommunikáció. [8], [9], [10], [11]

4.2. Sweep zavarás a teljes sávartományban

A második lehetséges zavarási mód, amikor a vizsgált sávartományon végig halad a zavarjelünk. Ennél a zavarási módnál fontos meghatározni a zavarjel sávszélességét, illetve a sweep idejét. A sweep idő lényeges, mivel ha nagyon lassan halad a jelünk, akkor a kommunikáció továbbra is megfelelő lehet, viszont kellően gyors sweep estén már részleges vagy akár teljes zavarás bekövetkezhet. [8], [9], [10], [11]

4.3. Teljes sávartomány zavarása

A harmadik lehetséges zavarási mód, amikor a vizsgált sávartományt teljesen lefedjük a zavarjelünkkel. Érdemes a teljes sávot úgy lefedni, hogy túlnyúljon a zavarni kívánt tartományon, mivel így biztosan zavarjuk az egész sávot. Ennél a zavarási típusnál biztos eredményt tudunk elérni a sávartományi zavarásban. [8], [9], [10], [11]

5. Zavarás megvalósítása SDR berendezéssel

A sáv tartományi zavarást SDR (Software Defined Radio), berendezéssel fogom a végezni, amelyet a GNU Radio nevű alkalmazással fogok vezérelni. Vizsgálataimban a GNU Radio 3.10-es verziót fogom használni. A Zavarásokat pedig spektrumanalizátor segítségével fogom nyomon követni.

Az SDR (Software Defined Radio) magyar megfelelője a szoftverrádió. Olyan rendszereket foglal magában, ahol rádiófrekvenciás hardverekkel jelfeldolgozási műveleteket hajtunk végre. Számos SDR eszköz megtalálható az interneten pendrive vagy akár kisebb dobozos kivitelben is. A mérések során az Ettus USRP B210-es eszközt használom, ami egy két csatornás adó-vevővel van ellátva. Az eszköz frekvencia lefedettsége 70 MHz-től 6 GHz-ig terjed. Kifejezetten kutatási területekre tervezték. A fő előnye, hogy kompakt egyszerű az összeköttetése laptoppal vagy számítógéppel, illetve antennákkal. A mérések során a GNU Radio programot használom, amelyen keresztül vezérelni tudom az eszközünket. [12]



3. ábra: Ettus USRP B210

Forrás: <https://www.ettus.com/all-products/ub210-kit/>

A GNU Radio program mindenki számára ingyenes és használhatósága új tereket nyit meg a szoftver vezérelt rádiók világában. Fontos megemlíteni, hogy nem karakteres írott programozást kell végrehajtanunk egyes feladatok elvégzéshez, hanem blokkokból tudjuk elkészíteni az általunk tervezett környezetet. Az egyes blokkok között egyszerűen tudunk összeköttetést készíteni, és beállítani az általunk kiszámolt és meghatározott követelményeket (értékeket). Ebből kiindulva bármikor állítható bármelyik paraméter, természetesen ameddig a fizikai eszközünk hardveres specifikációja azt engedi. A későbbiekben látható, hogy mind a három zavarási módhoz külön blokkvázlat tartozik, valamint az esetleges módosításoknál használt blokkokat és azok összeköttetéseit, illetve paramétereiket kell változtatni, amennyiben szükségem lesz rá. A vizsgálatok ismertetésénél részletesen kitérek az egyes beállításokra. [13]

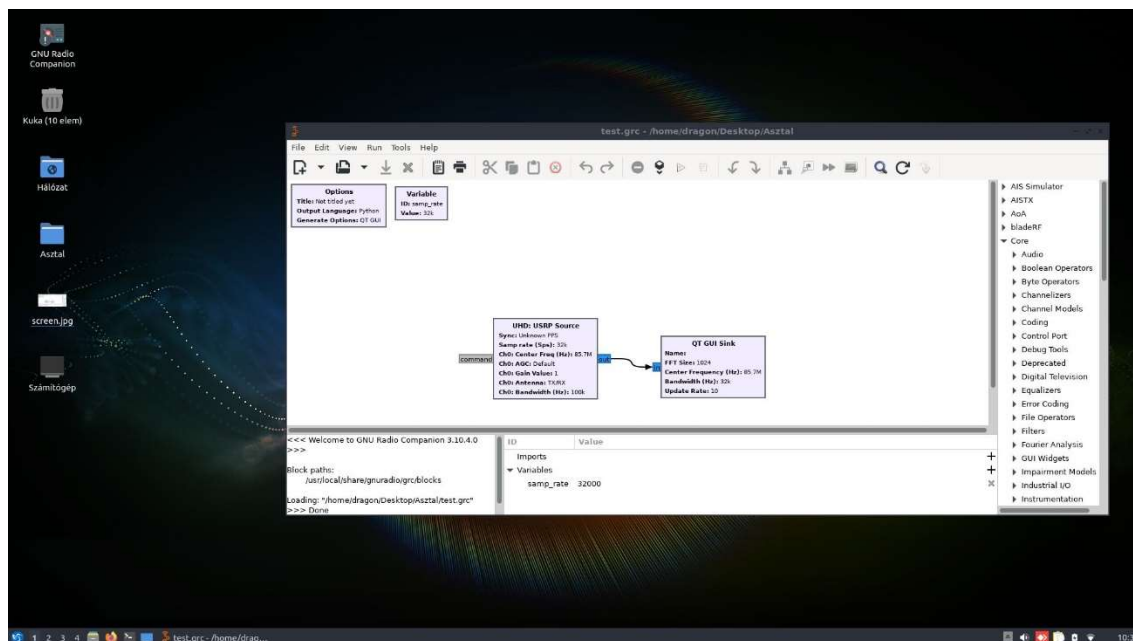


4. ábra: GNU Radio Logo

Forrás: <https://www.gnuradio.org/>

A GNU Radio program legújabb verziója a 3.10-es kiadás. Amelyet lehetőségünk van telepíteni macOS, Windows, Ubuntu, Fedora, Debian, Raspberry Pi OS és Linux Mint rendszerekre is. A telepítés menete a gyártói honlapon elérhető és a részletesen dokumentált útmutatókkal könnyedén elvégezhető. A kutatásom során viszont egy számomra kedvezőbb alternatívát választottam operációs rendszer platformnak, amelyben már előre implementálásra kerültek főbb alkalmazások, programok, mint például a GNU Radio is. Az operációs rendszer neve DragonOS, amely egy speciális Ubuntu rendszer melyben csak a legszükségesebb egységek találhatók meg. A rendszer tárterület igénye 20 GB így egy másik operációs rendszer mellé is fel tudjuk telepíteni. Továbbá lehetőségünk van Live verzióban is futtatnia a rendszert egy legalább 4GB-os pendriveről. Előre definiált alkalmazások terén számos szoftver vezérelt rádióhoz kapcsolódó alkalmazás érhető el, amelyek az operációs rendszer honlapján megtalálható.

További kutatásom során nagy segítségemre lesz a rendszer, mivel rengeteg alkalmazás és eszköz érhető el számomra, amelyekkel még mélyebben tudom megismerni és vizsgálni a tématerületet. Az 5. ábrán látható a DragonOS operációs rendszer főképernyője.



5. ábra: DragonOS főképernyője

Forrás: Saját szerkesztés

A spektrumanalizátorok a frekvencia tartományban képesek a jeleket megjeleníteni, ami oszcillátorok, modulátorok, demodulátorok, mobil hálózatok frekvencia tartományban történő méréseire és műholdrendszerek frekvencia tartományi méréseiben alkalmazható. A vizsgálataim során elengedhetetlen a berendezés használata, mivel folyamatosan nyomon kell követni a sávtartományi változásokat. Fontos megemlíteni, hogy számos más területen is alkalmazható a spektrumanalizátor. [14]

Ilyen terület lehet például:

- vezeték nélküli kommunikációs technológiák (Wi-Fi, NFC, Bluetooth)
- teljesítményerősítők tesztelése
- 3GPP technológiák fizikai réteg szintű tesztelése
- BTS és UE transmitter tesztek
- Stb.

Az összeállítások során egy Anritsu MS2090A típusú spektrum és jelanalizátor segítségével fogom a vizsgálatokat elvégezni. Az eszköz megfelelően használható a sávtartományok vizsgálatára, mivel 9 kHz-től 9 GHz-ig képes vizsgálni a frekvencia tartományt. Az eszköz képe a 6. ábrán látható.



6. ábra: Anritsu MS2090A spektrum és jelanalizátor

Forrás: <https://www.anritsu.com/en-us/test-measurement/products/ms2090a>

5.1. Zavarvizsgálatok megtervezése, kialakítása

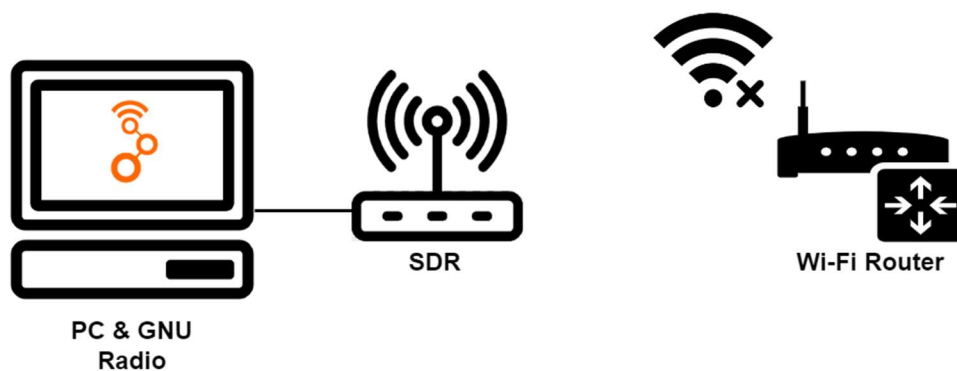
Miután meghatároztam, hogy milyen zavarási lehetőségeket fogok alkalmazni a vizsgálataim során (spot, sweep és teljes sáv zavarása), illetve a vizsgálatok során használandó eszközök és programok meghatározásra és telepítésre kerültek, elkezdtem megtervezni a lehetséges vizsgálati összeállításokat.

Első körben a kishatótávolságú technológiák vizsgálatát tűztem ki célul és ezen belül is a Wi-Fi és a Bluetooth technológiákat. A választásom fő oka, hogy ISM sávot használó technológiák a legnépszerűbbek az IoT szempontjából. Irodalomkutatásom során számos cikkben és gyártó adatlapok leírásában találkoztam az említett két technológiával. Ezeket a kommunikációs technológiákat olyan eszközök használják, mint az okos villanykörte, termosztát, ajtó zár és számos otthoni használatra készült berendezés. [15], [16], [17], [18]

A vizsgálatok kialakítását és tesztelését az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar Híradástechnika és Infokommunikáció Tanszék 5G laboratóriumában valósítom meg, ahol kontrollált körülmények között elvégezhetem az elsődleges teszteket.

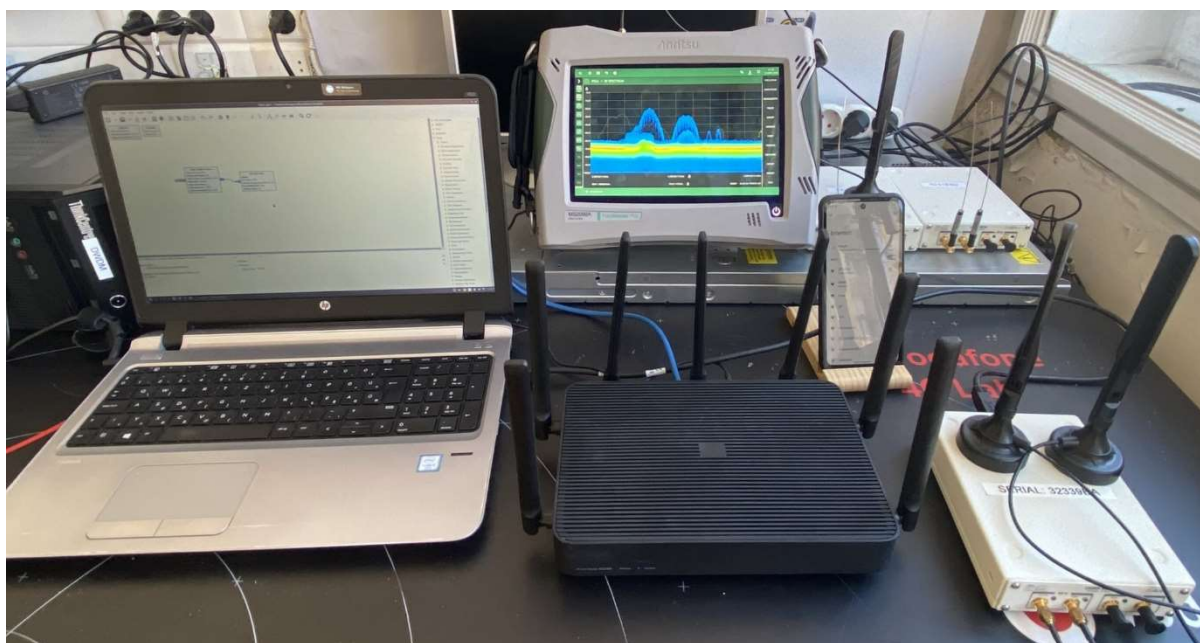
Az első zavarási vizsgálatomban egy alapvető háztartásban is megtalálható SOHO 2,4GHz-es Wi-Fi router a zavarni kívánt eszköz. A vizsgálati összeállításban egy számítógép található, amelyre feltelepítésre került a DragonOS. A számítógépet 3.0 USB-n keresztül csatlakoztatom a szoftver vezérelt rádióhoz. A számítógépen pedig a rendszerben telepített GNU Radio szoftver segítségével vezérelhetővé válik az SDR. A másik oldalon pedig megtalálható az otthoni SOHO Wi-Fi router. Továbbá a majdani vizsgálat ellenőrzésére egy okos telefon fog

még segítségemre lenni, amellyel ellenőrizni tudom a hálózat működését. A vizsgálat elméleti összeállítása a 7. ábrán látható. A gyakorlati megvalósítása pedig a 8. ábrán. [15], [16]



7. ábra: Wi-Fi Router zavarása SDR-rel

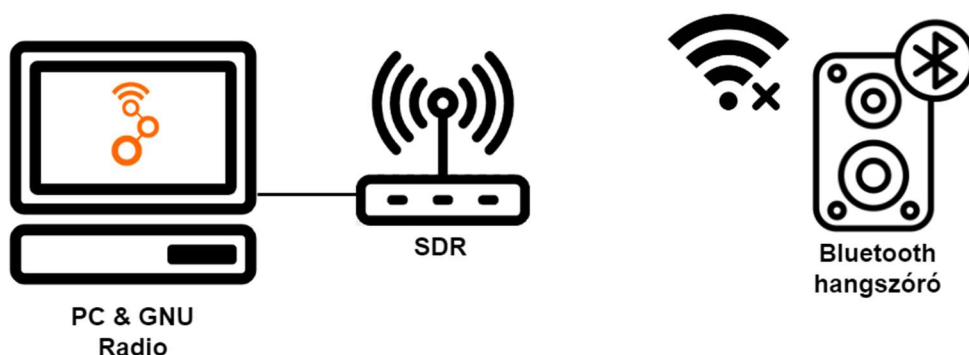
Forrás: Saját szerkesztés



8. ábra: Mérési környezet fizikai megvalósítása Wi-Fi

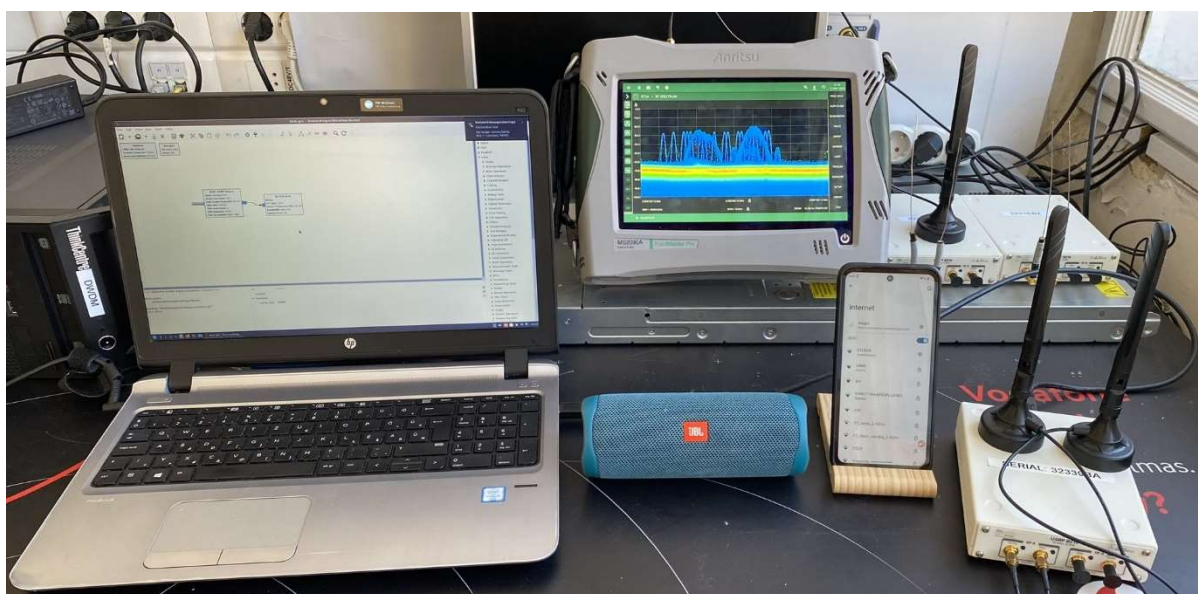
Forrás: Saját szerkesztés

A második vizsgálatban egy Bluetooth-os hangszóró lesz a zavarni kívánt eszköz. Természetesen más e technológiát használó eszköz is lehetne a zavarni kívánt eszköz, mint például mobiltelefonok adatküldés közben, vezeték nélküli fül- és fejhallgató, más eszközök is. A rendelkezésre álló eszközök szempontjából ez a megoldás volt a legkézenfekvőbb. A mérési összeállítás hasonló az első vizsgálathoz: a számítógép csatlakoztatásra kerül egy SDR berendezéssel és a számítógépről tudjuk vezérelni az SDR-t. A másik oldalon viszont egy vezeték nélküli hangszóró található, amelyen vizsgálat közben egy hang állomány kerül lejátszásra, így ha bármilyen eltérést hallunk a lejátszott hang állományban, akkor eredményes az alkalmazott zavarási mód. A vizsgálat elméleti összeállítása a 9. ábrán látható. A gyakorlati megvalósítása pedig a 10. ábrán. [18]



9. ábra: Bluetooth hangszóró zavarása SDR-rel

Forrás: Saját szerkesztéssel



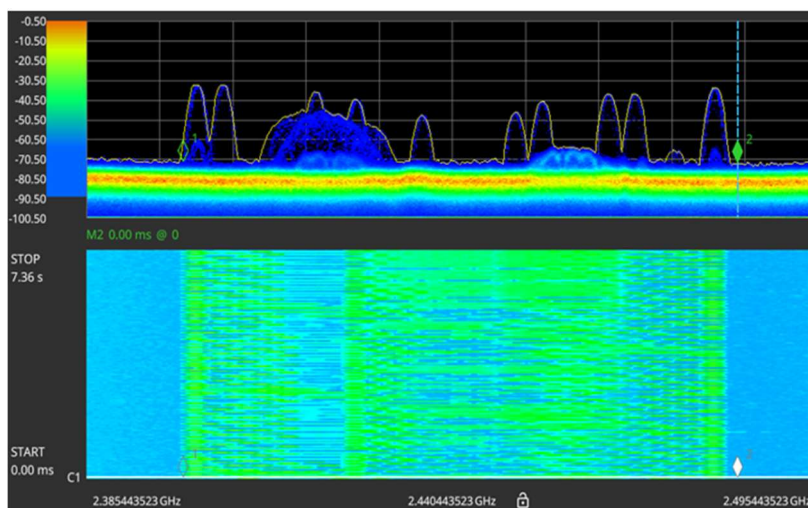
10. ábra: Mérési környezet fizikai megvalósítása Bluetooth

Forrás: Saját szerkesztés

A vizsgálatok alatt folyamatosan ellenőrzésre fog kerülni a frekvencia tartományban történő zavarás. Az ellenőrzéshez az Anritsu MS2090A típusú spektrum és jelanalizátor fog segítségemre lenni, mely által az általános spektrumképet tudom vizsgálni, illetve az előző fejezetben említett három fajta zavarási módot, mint a spot, sweep és a teljes sávtartományi zavarásokat tudom ellenőrizni.

5.2. Zavar vizsgálatok tesztelése

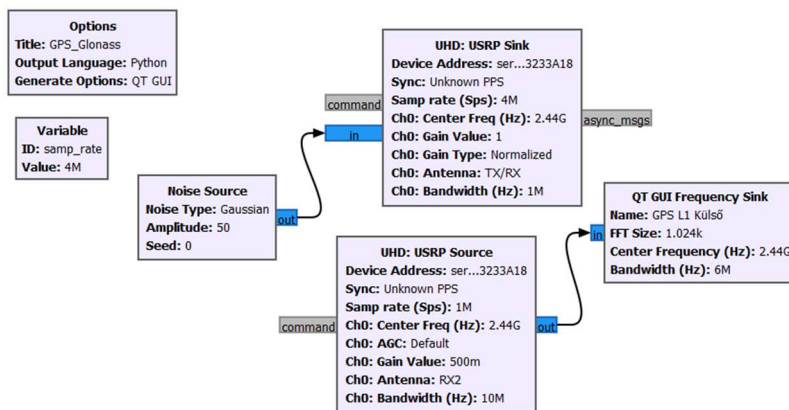
A vizsgálatok megkezdése előtt fontos felmérni az ISM frekvencia sávot spektrumanalizátor berendezéssel. Ez az első lépés, mivel így tudom majd viszonyítani az egyes zavarási típusokat. Megvalósítást tekintve bekapcsoltam az Anritsu MS2090A típusú spektrum és jelanalizátort kiválasztottam a spektrumanalizátor funkciót és beállítottam az ISM sávot, amely 2,4 GHz - 2,4835 GHz-ig tart. Az ISM sáv spektruma a 11. ábrán látható.



11. ábra: ISM sáv spektrum képe

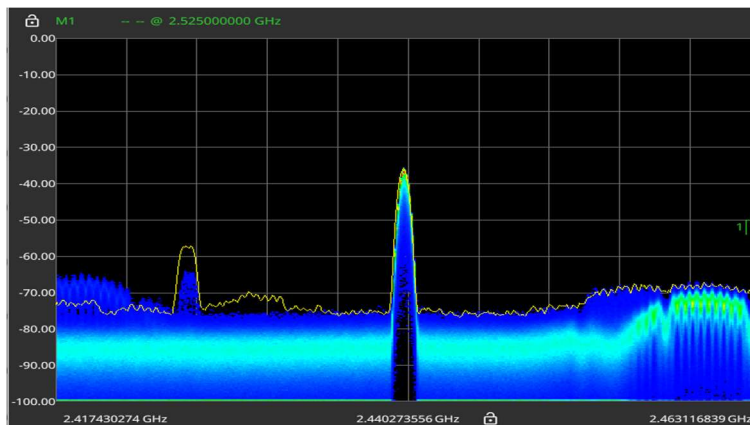
Forrás: Saját szerkesztés

Az első vizsgálatomban a spot zavarást valósítottam meg az ISM sáv elején, közepén és végén. A vizsgálataim során sem a Bluetooth-os hangszóró, sem pedig a Wi-Fi-s hálózatban nem tapasztaltam semmiféle változást vagy akadozást. A 12. ábrán látható a zavarás blokk vázlata, amelyen a 2,44GHz-es frekvenciára került beállításra a center frekvencia és Gaussian noise a zavarforrás.



12. ábra: Spot zavarás SDR blokk vázlata

Forrás: Saját szerkesztés



13. ábra: Spot zavarás spektrum képe

Forrás: Saját szerkesztés

A második vizsgálatom során a sweep zavarást teszteltem. A zavarás megvalósításához szükségem volt egy egyszerű Python script-re, amely segítségével pontos megadható, hogy melyen tartományban és mekkora lépésekkel kerüljön kisugárzásra a zavarás. A Python script a 14. ábrán látható.

```
# this module will be imported in the into your flowgraph
f1 = 2400000000
f2 = 2485300000
f = f1

step = 1000000

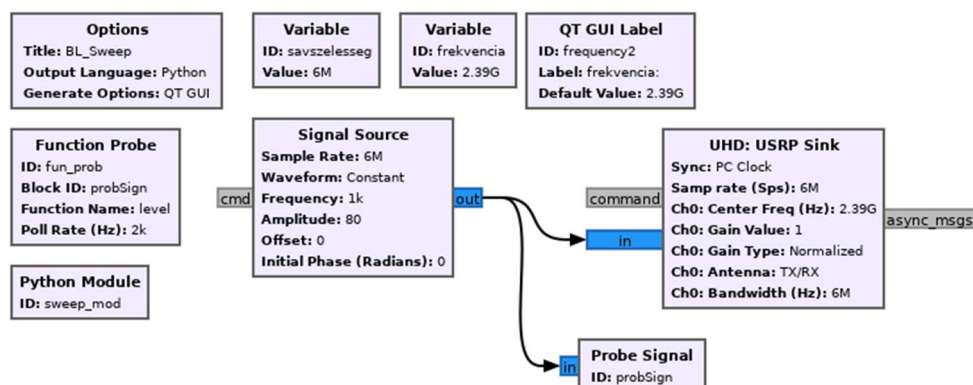
def sweeper(prob_lvl):
    global f1,f2,f,step
    if prob_lvl:
        f +=step
    if f>=f2:f=f1

    return f
```

14. ábra: Python script kódsora

Forrás: Saját szerkesztés

Az f1 és f2 értékekkel állítottam be azt a határt, amely között megvalósuljon a sweep. A step változóban megadtam a sweep léptékét. A mi esetünkben a tartomány a már ismertett ISM sáv és ebben a tartományban 1 MHz-enként történik a lépés, így egy folytonos sweep-et kaptam. Azért állítottam 1 MHz-re a léptéket, mert a Bluetooth Classic az ISM a tartományon belül 79 darab 1 MHz-es sáv szélességű csatornát hoz létre. Viszont Bluetooth Low Energy eszközök esetében 2 MHz-re kell módosítani, mivel ennél a technológiánál 40 darab 2 MHz-es csatorna került kialakításra. A script megfelelő paraméterezése után a GNU Radio-ban létrehoztam a modellt a szükséges blokkok felhasználásával, amely a 15. ábrán látható.



15. ábra: Sweep zavarás SDR blokk vázlata

Forrás: Saját szerkesztés

A megfelelő paraméterek megadása után teszteltem is a zavarást, melyre a 16. ábrán látható spektrum képet kaptam, amelyen jelöltem a sweep irányát.

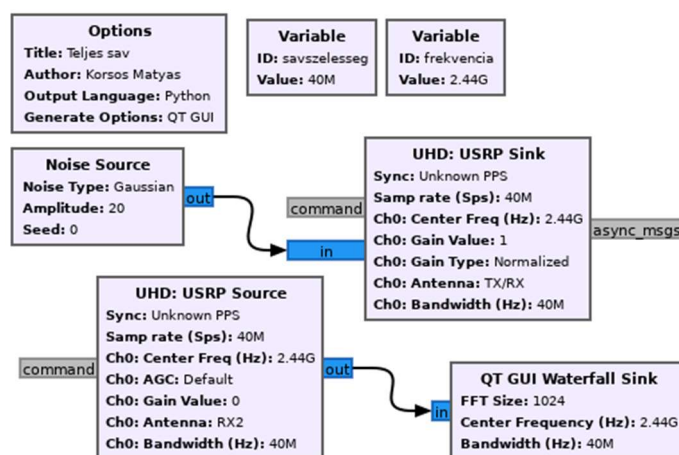


16. ábra: Sweep zavarás spektrum képe

Forrás: Saját szerkesztés

A sweep zavarás sikeresnek mondható, mivel a lejátszott hang állomány szakadozott, illetve a Wi-Fi hálózat-on a mobiltelefonon lassabban töltötte be ugyan azt a weboldalt, ami a zavarás előtt szinte azonnal elérhető volt. A zavarás során csomagvesztést nem vizsgáltam.

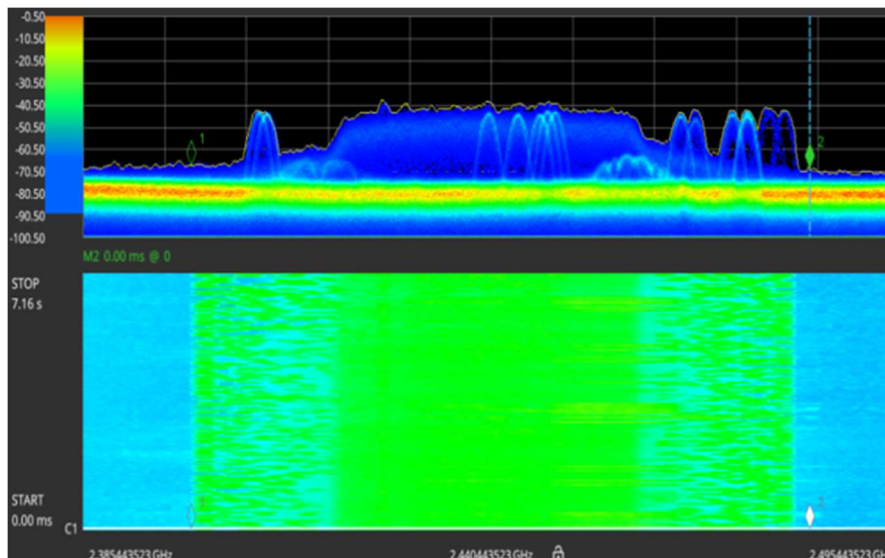
A harmadik vizsgálatom során az egész ISM sávot zavartam. Center frekvenciára megadtam a sáv tartomány közepét 2,44GHz-et. A sáv tartományi közéértékhez képest mind két oldalra beállítottam a 40MHz-es sáv szélességet így „lefedettnek” mondható a vizsgált sáv. A használt zajforrásom ez esetben Gaussian noise. A beállított paraméterek a 17. ábrán láthatóak.



17. ábra: Teljes sáv zavarásának SDR blokk vázlata

Forrás: Saját szerkesztés

A beállított paraméterek után elindítottam a zavarást. A zavarás a paraméterek szerinti formában jelent meg, amely a 18. ábrán látható. Viszont az is látszik, hogy nem fedi le teljes amplitúdóban a spektrumot ez a berendezés határai miatt látszódik így érdemes lesz majd a későbbi vizsgálatok során két részre bontania a zavarást, hogy ne egy zavarjellel próbáljam lefedni a teljes sávtartományt. Zavarás közben teljesen megszakadt a Wi-Fi és a Bluetooth kapcsolat az eszközök között is.



18. ábra: Teljes sávtartomány zavarásának spektrum képe

Forrás: Saját szerkesztés

Tapasztalataimat az első körös vizsgálatok után a 3. táblázatban foglaltam össze. Nagyon fontos megjegyezni, hogy a mérések során rengetek hasznos tapasztalatot gyűjtöttem a GNU Radio-val és az egyes paraméterek megadásával kapcsolatban. A tapasztalatok alapján javítani fogom a zavaró állományokat és egy konkrétan meghatározott és már nem módosított forma vizsgálat alapján fogom elvégezni a vizsgálatok különböző IoT eszközökön, hogy hogyan is viselkednek SDR-es zavarás hatására. Összeségben elmondható, hogy az előzetes vizsgálatok alapján a sweep és a teljes sávtartomány zavarása lesz a megfelelő zavarási mód, de a spot zavarást sem vettem el. Eredményeim összefoglalása a 3. táblázatban látható.

	Zavarás a sáv elején, közepén és végén	Sweep zavarás	Teljes sáv zavarása
Wi-Fi	X	✓	✓
Bluetooth	X	✓	✓

3. táblázat Zavarvizsgálati eredmények összefoglalása

Forrás: Saját szerkesztés

6. Továbbfejlesztési lehetőségek

A megtervezett vizsgálatokat, továbbá a dolgozatomat számos továbbfejlesztési lehetőséggel szeretném kiegészíteni a közeljövőben, hogy még részletesebben bemutathassam a tématerületet.

A megtervezett és tesztelt vizsgálatokat szeretném kiegészíteni a szerzett tapasztalatok alapján és mind a három zavarási vizsgálatot részletesen dokumentálni és kiértékelni, továbbá egy komplex összehasonlítást készíteni, hogy melyik zavarási mód a leghatásosabb az egyes eszközöknél. Ezen kívül pedig még több otthonainkban is megtalálható IoT eszközt megvizsgálni, hogy még részletesebb vizsgálati eredményeim születhessenek. Ilyen IoT eszközök lehetnek a Sonoff kapcsolók, kávéfőzők, termosztátok, Google, Amazon, illetve az Apple eszközei.

Az Egyetem Villamosmérnöki Karának Híradástechnika és Infokommunikáció Tanszéken megvalósuló kísérleti vezeték nélküli hálózaton a közeljövőben valós sérülékenységi vizsgálatokat tudok végezni. A hálózat MikroTik routerek és access pointokból fog felépülni, amely így egy nagyobb otthoni vagy céges kisvállalati hálózatokhoz hasonlít majd. Az új hálózat bemutatása a következő tudományos diákköri dolgozatom jelentős részét fogja képezni az új vizsgálatok ismertetése mellett. Az új vizsgálatok során célom több hálózati paraméter mérése, amelyek részletesebben alátámasztják kísérleteimet.

7. Összefoglaló

A tudományos munkámban részletesen bemutattam az IoT elgondolását. Röviden összefoglaltam a tématerületet. Bemutatásra került az IoT elődje az M2M, illetve az ipari felhasználása a technológiának, mint az IIoT.

Munkában összegyűjtöttem az IoT technológiákat kiterjedésük szerint, mint nagy és kis kiterjedésű hálózatok és utóbbi technológiáit, a Bluetooth, Wi-Fi, RFID, NFC és a Zigbee, Matter-t. Ezeket a technológiákat megvizsgáltam frekvenciatartomány szempontjából, a szabványok részéről, a hálózati struktúrájuk alapján, az adatsebesség terén és a hatótávolság szempontjából. Ezek a jellemzők fontosak a jövőbeni zavarvizsgálatok miatt.

Megvizsgáltam az alapvető biztonsági és sérülékenységi kérdéseket az IoT-vel kapcsolatban, mind szoftveres, mind fizikai szempontból. A tervezett vizsgálataimban a fizikai szempontból megközelíthető zavarási módokat veszem alapul. Bemutattam a vizsgálatokhoz elengedhetetlen eszközöket - az Ettus B210-es USRP SDR berendezés DragonOS operációs rendszert, illetve az Anritsu MS2090A típusú spektrum és jelanalizátor - és a szoftvert - a GNU Radio 3.10-es verzióját.

Két vizsgálati összeállítást valósítottam meg, amelyekkel megfelelően tudtam szimulálni és vizsgálni a zavarási módszereket. Az egyik vizsgálati összeállítás alapjának egy otthoni környezetben is megtalálható SOHO Wi-Fi routert választottam, míg a másik esetben pedig egy általános Bluetooth-os hangszórót. A későbbiekben célom megvizsgálni más IoT eszközök sérülékenységét.

Összességében, a dolgozatom betekintést biztosít napjaink egyik leggyorsabban bővülő technológiáiba az IoT és IIoT-be. Továbbá bemutatja a fizikai zavarási módok alapvető formáit és kivitelezési lehetőségeit gyakorlati vizsgálatokon keresztül.

8. Rövidítésjegyzék

Az alábbi táblázat segítséget nyújt dokumentumban található rövidítések könnyebb megértéséhez, elsajátításához.

Rövidítés	Angol megnevezés	Magyar megnevezés
IoT	Internet of Things	Dolgok internete
RFID	Radio Frequency Identification	Rádiófrekvenciás azonosítás
ITU	International Telecommunication Union	Nemzetközi Távközlési Unió
M2M	Machine to Machine	Eszköz az eszközzel
IIoT	Industrial Internet of Things	Dolgok iparai internete
H2H	Human to Human	Ember az emberrel
H2T	Human to Thing	Ember a dolgokkal
T2T	Thing to Thing	Dolgok a dolgokkal
NMHH	National Media and Infocommunications Authority	Nemzeti Média és Hírközlési Hatóság
WAN	Wide Area Network	Nagy kiterjedésű hálózatok
LPWAN	Low Power Area Network	Alacsony energiaigényű, nagy hatótávolságú hálózat
LAN	Local Area Network	Helyi hálózat
WLAN	Wireless Local Aarea Networ	Vezeték nélkül helyi hálózat
PAN	Personal Area Network	Személyi hálózat
NFC	Near Field Communication	Rövid hatótávú kommunikáció
GSM	Global System for Mobile communication	
LTE	Long-Term Evolution	„Hosszútávú fejlődés”

5G	Fifth Generation	Ötödik generációs mobilhálózat
Nb-IoT	NarrowBand-Internet of Things	Keskenysávú dolgok internete
LTE-M	Long Term Evolution for Machines	
NTN-IoT	None-Terrestrial Networks	Nem földfelszíni hálózatok IoT
3GPP	Third Generation Partnership Project	Harmadik Generációs Partnerségi Projekt
IEEE	Institute of Electric and Electronic Engineers	
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
LF	Low Frequency	Hosszúhullám
HF	High Frequency	Magas frekvencia
UHF	Ultra High Frequency	Deciméteres hullám
ISM	Industrial, Scientific, and Medical	Ipari, tudományos és orvosi
SDR	Software Defined Radio	Szoftver vezérelt rádió
USB	Universal Serial Bus	Univerzális soros busz
SOHO	Small Office, Home Office	Otthoni Irodai, kisvállalati
Wi-Fi	Wireless Network	Vezeték nélküli mikrohullámú kommunikáció
BTS	Base Transceiver Station	Bázis adó-vevő állomás
UE	User Equipment	Felhasználói készülék

9. Irodalomjegyzék

9.1. Források

[1] ITU Internet Reports: The Internet of Things 2005 Online,

Link: <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>

(Letöltve: 2023. szeptember 13.)

[2] Nemzeti Kibervédelmi Intézet: IoT eszközök biztonsági kérdései - Az ipar, 2022 Online,

Link: https://nki.gov.hu/wp-content/uploads/2022/09/IoT-eszkozok-biztonsagi-kerdesei_II_CTI_jelentes.pdf

(Letöltve: 2023. szeptember 13.)

[3] Sudhir Sharma, Bharat Bhushan, Narayan C. Debnath: Security and Privacy Issues in IoT Devices and Sensor Networks, ELSEVIR ACADEMIC PRESS, 2020 Online,

Link: <https://shop.elsevier.com/books/security-and-privacy-issues-in-iot-devices-and-sensor-networks/sharma/978-0-12-821255-4>

(Letöltve: 2023. szeptember 20.)

[4] Vlasios Tsiatsis, Stamatis Karnouskos, Jan Holler, David Boyle, Catherine Mulligan: Internet of Things, ELSEVIR ACADEMIC PRESS, 2018 Online,

Link: <https://shop.elsevier.com/books/internet-of-things/holler/978-0-12-407684-6>

(Letöltve: 2023. szeptember 20.)

[5] Muhammad Azhar Iqbal, Sajjad Hussain, Huanlai Xing, Muhammad Imran: IoT Security, WILEY, 2020 Online,

Link: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119701460>

(Letöltve: 2023. szeptember 20.)

[6] Nemzeti Kibervédelmi Intézet: IoT eszközök biztonsági kérdései - Az okosotthon, 2022 Online, Link: https://nki.gov.hu/wp-content/uploads/2022/09/IoT-eszkozok-biztonsagi-kerdesei_I_CTI_jelentes.pdf

(Letöltve: 2023. szeptember 13.)

[7] Nemzeti Kibervédelmi Intézet Otthoni hálózatok biztonsága, 2022 Online, Link: https://nki.gov.hu/wp-content/uploads/2022/09/Otthoni-halozatok-biztonsaga_CTI_jelentes.pdf

(Letöltve: 2023. szeptember 13.)

- [8] P.J. Varga, T. Wüthrl, S. Gyányi, M.T. Baross, A. Németh, “Jamming Attacks in 5G NR FR1,” 5th IEEE International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE 2022), pp. 175-180, 2022. Online,
Link: <https://ieeexplore.ieee.org/document/10046381>
(Letöltve: 2023. szeptember 13.)
- [9] Haig Zsolt, Kovács László, Ványa László, Vass Sándor: Elektronikai hadviselés, Nemzeti Közszerálatali Egyetem Hadtudományi és Honvédtisztképző Kar, 2014 Online,
Link: <https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/100390>
(Letöltve: 2023. szeptember 13.)
- [10] Hossein Pirayesh, Huacheng Zeng: Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey, IEEE Communications Surveys & Tutorials Volume: 24 Issue: 2, 2022 Online, Link: <https://ieeexplore.ieee.org/document/9733393>
(Letöltve: 2023. szeptember 13.)
- [11] Marc Lichtman, Jeffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer, Jeffrey H: A communications jamming taxonomy, IEEE Security & Privacy Volume: 14 Issue: 1, 2016 Online,
Link: <https://ieeexplore.ieee.org/document/7397710>
(Letöltve: 2023. szeptember 13:)
- [12] Tóth Károly: Információfeldolgozás USRP platformon, BME Méréstechnika és Információs Rendszerek Tanszék, 2018 Online,
Link: <http://dsp.mit.bme.hu/userfiles/szakdolgozat/tothkszakdolgozat18.pdf>
(Letöltve: 2023. október 2.)
- [13] Nguyen B.Truong, Young-Joo Suh, Chansu Yu: Latency Analysis in GNU Radio/USRP-based Software Radio Platforms, IEEE Military Communications Conference, 2013 Online,
Link: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6735640>
(Letöltve: 2023.október 2.)
- [14] Szűcs László: Műszerismertető segédlet, BME Villamosmérnöki és Informatikai Kar, 2008 Online,
Link: <https://www.mit.bme.hu/system/files/oktatas/targyak/10878/muszer10.pdf>
(Letöltve: 2023.október 2.)

[15] Zsolt Haig, Zsolt Illési, János Péter Varga: Possibilities of Electronic Jamming of WLAN Networks in the Physical Layer, Hadmérnök, 17. évfolyam 3. szám, pp.133-152., 2022 Online, Link: <https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/6248/5161>

(Letöltve: 2023.október 4.)

[16] T. Karhima, A. Silvennoinen, M. Hall, S.-G. Haggman: IEEE 802.11b/g WLAN tolerance to jamming, IEEE MILCOM 2004. Military Communications Conference, 2004 Online, Link: <https://ieeexplore.ieee.org/document/1495141/authors#authors>

(Letöltve: 2023.október 4.)

[17] Péter János Varga, Zsolt Illési: WI-FI 6 APPLICATION IN IOT ENVIRONMENT, Interdisciplinary Description of Complex Systems 20 (3) pp.277-283., 2022 Online, Link: <https://www.indecs.eu/2022/indecs2022-pp277-283.pdf>

(Letöltve: 2023.október 4.)

[18] Volodymyr Sokolov, Pavlo Skladannyi, Volodymyr Astapenya: Bluetooth Low-Energy Beacon Resistance to Jamming Attack, IEEE 13th International Conference on Electronics and Information Technologies (ELIT), 2023 Online,

Link: <https://ieeexplore.ieee.org/document/10310815>

(Letöltve: 2023.október 4.)

9.2. Ábrák

1. ábra: IoT technológia kezdeti elképzelése Forrás: Saját szerkesztés, <https://cutt.ly/ywQZ9pAh> alapján (Oldalszám: 4.)
2. ábra: M2M és IoT strukturális összehasonlítása Forrás: Saját szerkesztés (Oldalszám: 5.)
3. ábra: Ettus USRP B210 Forrás: <https://www.ettus.com/all-products/ub210-kit/> (Oldalszám: 13.)
4. ábra: GNU Radio Logo Forrás: <https://www.gnuradio.org/> (Oldalszám: 14.)
5. ábra: DragonOS fő képernyője Forrás: Saját szerkesztés (Oldalszám: 15.)
6. ábra: Anritsu MS2090A spektrum és jelanalizátor Forrás: Forrás: <https://www.anritsu.com/en-us/test-measurement/products/ms2090a> (Oldalszám: 16.)
7. ábra: Wi-Fi Router zavarása SDR-rel Forrás: Saját szerkesztés (Oldalszám: 17.)
8. ábra: Mérési környezet fizikai megvalósítása Wi-Fi Forrás: Saját szerkesztés (Oldalszám: 17.)
9. ábra: Bluetooth hangszóró zavarása SDR-rel Forrás: Saját szerkesztés (Oldalszám: 18.)
10. ábra: Mérési környezet fizikai megvalósítása Bluetooth Forrás: Saját szerkesztés (Oldalszám: 18.)
11. ábra: ISM sáv spektrum képe Forrás: Saját szerkesztés (Oldalszám: 19.)
12. ábra: Spot zavarás SDR blokk vázlata Forrás: Saját szerkesztés (Oldalszám: 20.)
13. ábra: Spot zavarás spektrum képe Forrás: Saját szerkesztés (Oldalszám: 20.)
14. ábra: Python script kódsora Forrás: Saját szerkesztés (Oldalszám: 21.)
15. ábra: Sweep zavarás SDR blokk vázlata Forrás: Saját szerkesztés (Oldalszám: 21.)
16. ábra: Sweep zavarás spektrum képe Forrás: Saját szerkesztés (Oldalszám: 22.)
17. ábra: Teljes sáv zavarásának SDR blokk vázlata Forrás: Saját szerkesztés (Oldalszám: 22.)
18. ábra: Teljes sáv tartomány zavarásának spektrum képe Forrás: Saját szerkesztés (Oldalszám: 23.)

9.3. Táblázatok

1. táblázat: IoT technológiák általános csoportosítása Forrás: Saját szerkesztés (Oldalszám: 8.)

2. táblázat: Kis hatótávolságú technológiák ismertetése Forrás: Saját szerkesztés (Oldalszám: 10.)

3. táblázat: Zavarvizsgálati eredmények összefoglalása Forrás: Saját szerkesztés (Oldalszám: 23.)

„A kulturális és innovációs minisztérium ÚNKP-23-2 kódszámú új Nemzeti kiválóság programjának a nemzeti kutatási, fejlesztési és innovációs alapból finanszírozott szakmai támogatásával készült.”

