Innovatív biztonsági technikák a 6G fizikai rétegében: THz, AI és kooperatív védelem

Gódor Győző
BME Hálózati Rendszerek és Szolgáltatások Tanszék
godorgy@hit.bme.hu

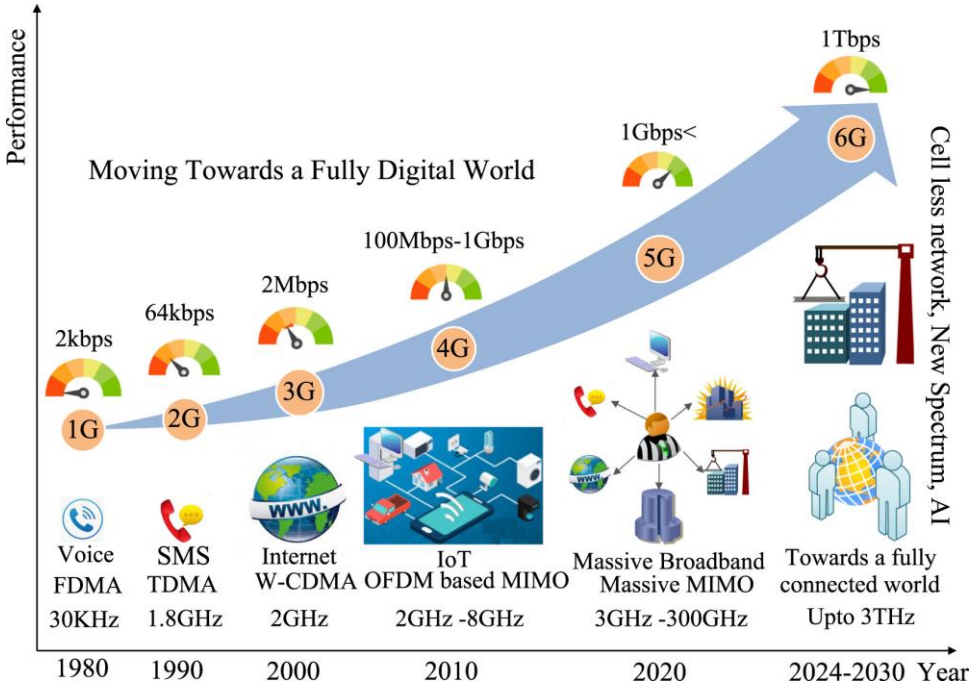
MŰEGYETEM 1782 | BME

MCL Mobile Communications & Quantum Technologies Lab.

HTE Infokom 2025
Esztergom, 2025. november 5.

Tartalom

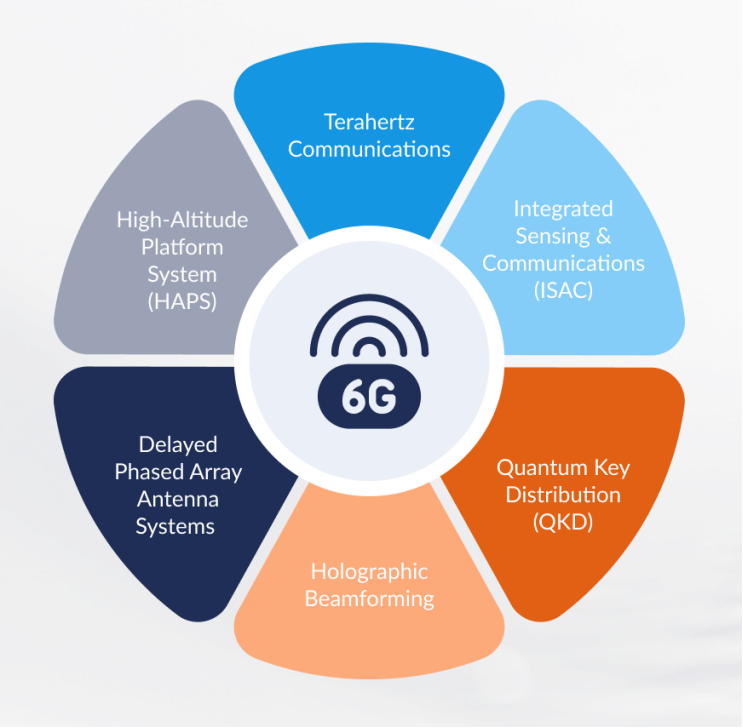
- 6G-ben megjelenő újítások
- Mi is az a fizikai réteg biztonság?
- 4G-5G biztonsági megoldások
- 6G fizikai réteg kihívások
- 6G fizikai réteg biztonsági megoldások
- Jövőbeli kutatási irányok



forrás: https://www.sciencedirect.com/science/article/pii/S1874490722001094

Bevezető – 6G-ben megjelenő újítások

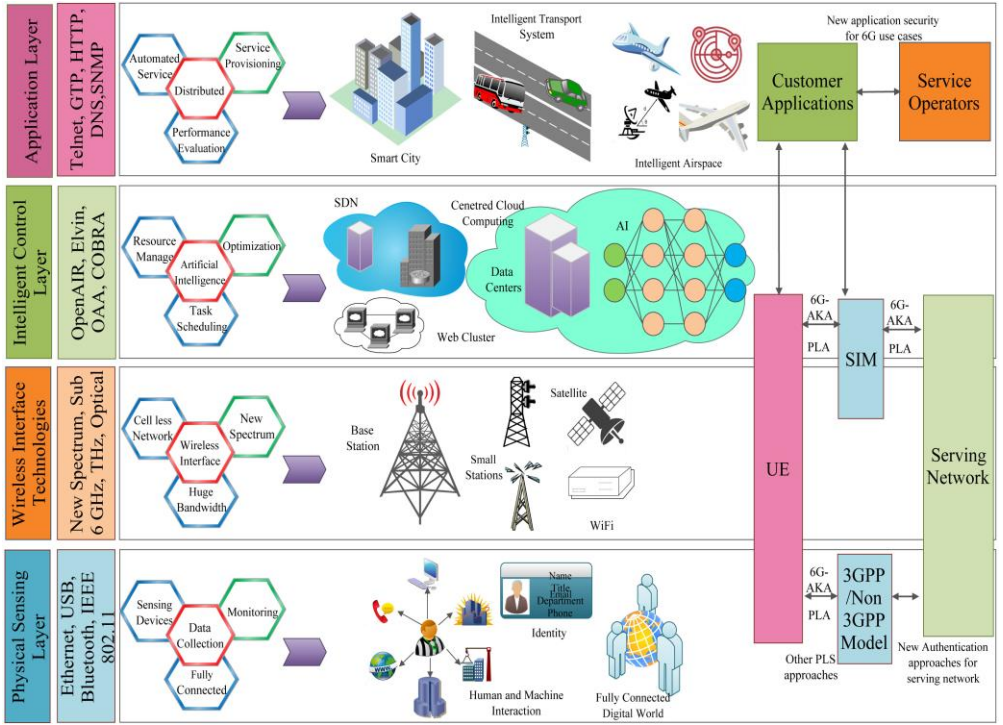
- Terrestrial és Non-Terrestrial Networks
- Új rádiósávok használata: mmWave, terahertz, optikai kommunikáció
- Mesterséges intelligencia (AI) és gépi tanulás (ML) alkalmazása
- Nagyon energiatakarékos és nagyon sűrűn elhelyezkedő eszközök: például in-body szenzorok és IoE eszközök



forrás: https://www.vationventures.com/research-article/the-road-to-6g-the-innovations-transforming-wireless-technology

Miért fontos a fizikai réteg biztonságával foglalkozni?

- Ez az „alap” réteg, melyre az összes többi réteg épül.
- A felsőbb rétegek megbízhatóságát és bizalmasságát biztosítja.
- Ha ezt a réteget támadás éri (pl. lehallgatás, hamis bázisállomás, jeltorzítás, zavarás), semmilyen magasabb szintű kriptográfiai vagy hitelesítési megoldás nem biztosít teljes védelmet.
- A klasszikus hálózati protokollok, titkosítási megoldások mellett a támadók egyre inkább magát a rádiós közeget célozzák.
- A 6G sikeréhez elengedhetetlen, hogy már a fizikai réteg szintjén is beépítsük a biztonságot.



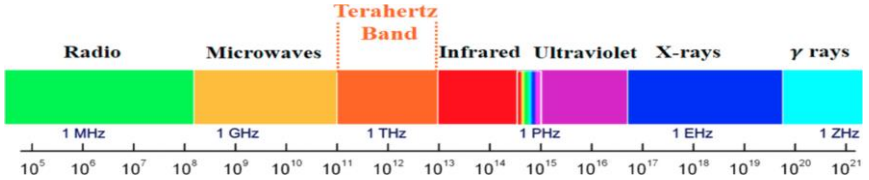
forrás: https://www.sciencedirect.com/science/article/pii/S1874490722001094

4G-5G fizikai réteg biztonsági megoldások fejlődése

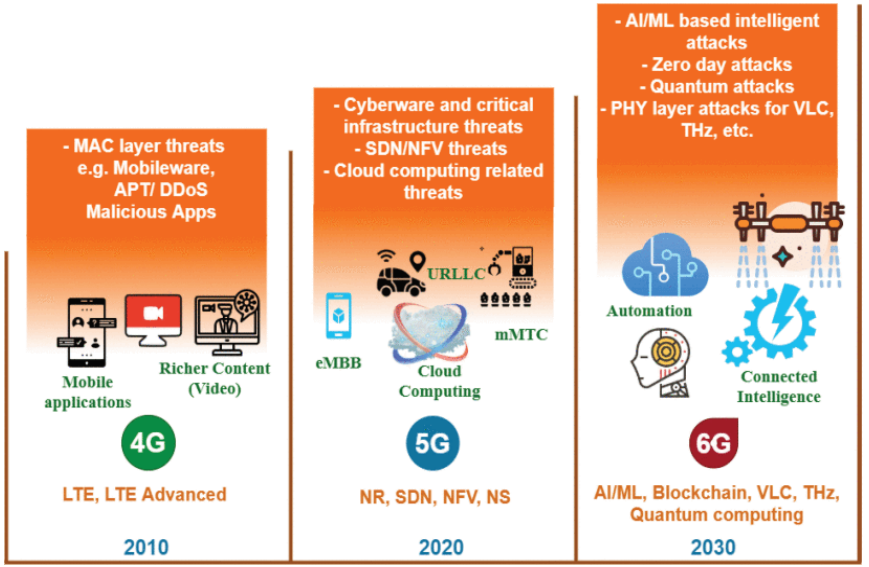
- 4G: kezdetleges PHY biztonsági megoldások
  - Jamming elleni védelem a fókuszban: frekvencia- és időugratás
  - Csatorna-alapú hitelesítés korlátozott mértékben: pl. Csatorna impulzusválasza, vagy RSSI alapján
- 5G: továbbfejlesztett PHY SEC megoldások
  - Massive MIMO és nyalábformálás: zavarás elleni védelem, hatékonyság
  - Egyedi kulcsgenerálás csatornajellemzők alapján: fizikai réteg szintű titkosítás (PLS)
- A PHY biztonsági megoldások korlátozottak, főként a csatornák lassú változása és a hardveres korlátok miatt.

Miért kell új fizikai réteg biztonság 6G-hez?

- 6G-nél új spektrumok (THz, mmWave): jelentősen gyorsabb és dinamikusabb csatornaváltozás, új támadási lehetőségek.
- IoT-eszközök rohamos terjedése, ultranagy sűrűségű hálózatok.
- Kvantum számítógépek hosszútávon a klasszikus titkosítást is fenyegetik.
- AI-alapú támadók: adaptív, tanuló támadás- és hamis adatgenerálás.
- A 6G-technológia ugrásszerű fejlődése új, eddig ismeretlen kockázatokat és kihívásokat hoz a fizikai réteg biztonságában.



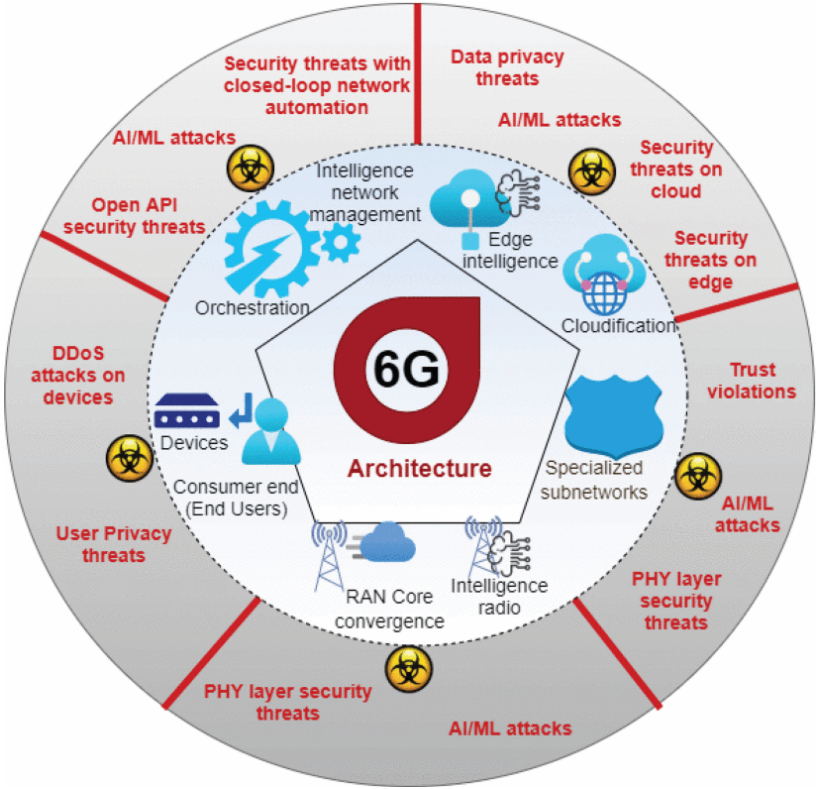
forrás: https://doi.org/10.1016/j.jnca.2024.104040



forrás: https://ieeexplore.ieee.org/document/9426946

6G fizikai réteg elleni támadások

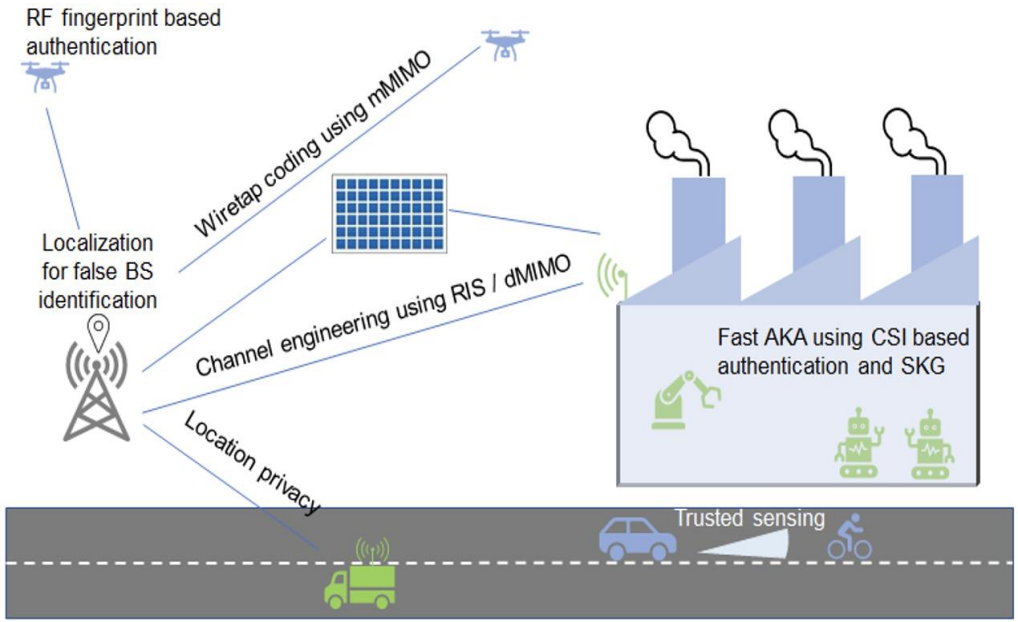
- Jamming:
  - THz sávban irányított vagy nagy teljesítményű blokkoló jelek
- Eavesdropping
- Spoofing
- AI/ML-alapú támadások:
  - gyorsan adaptálódnak a védekezéshez
  - mérgezik a csatornamodelleket



forrás: https://ieeexplore.ieee.org/document/9426946

6G fizikai réteg biztonsági követelmények

- Védelem a valós idejű jamming, eavesdropping és spoofing ellen.
- Csatorna információ alapú (CSI) hitelesítés és kulcsgenerálás valós környezetben.
- RF fingerprint alapú hitelesítés.
- Nagy megbízhatóság, késleltetéstűrés, privacy, forráshitelesítés.
- A vezeték nélküli csatorna fizikai tulajdonságainak aktív és intelligens változtatása programozható intelligens felületek (RIS) használatával.



forrás: https://www.eurecom.fr/publication/7731/download/comsys-publi-7731.pdf

Új technológiák a 6G fizikai réteg biztonságban

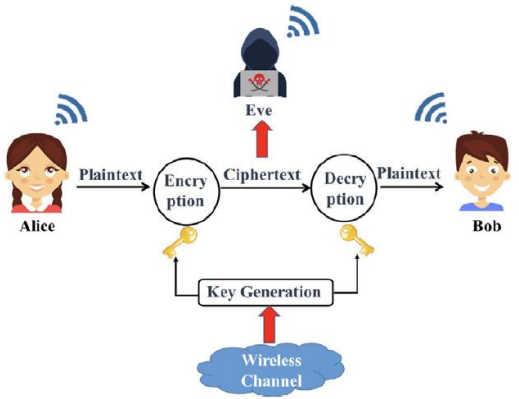
- Csatorna alapú (channel-based) hitelesítési protokollok: a fizikai réteg sajátos csatorna-jellemzőit (pl. CSI, CIR) használják fel hitelesítésre.
- Channel fingerprinting alapú megoldások: minden csatorna egyedi, mint ujjlenyomat – ez garantálja a megbízható hitelesítést.
- RF-fingerprinting: az eszköz saját rádiófrekvenciás lenyomata, pl. eszköz mikrohibái, IQ-imbalance.
- Quantum Key Distribution (QKD): kvantum alapú kulcsmenedzsment.
- AI-alapú támadás-felismerés, folyamatos tanuló védelem.

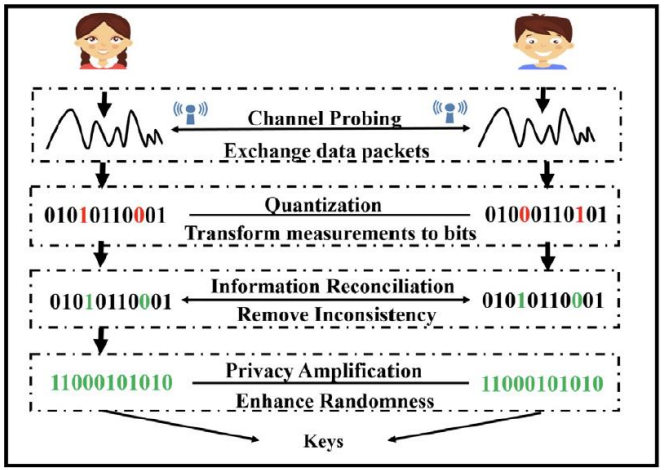
Példák: Csatorna alapú kulcselosztás

- Alice és Bob egymással kommunikálnak, a közös csatorna karakterisztikát használják a véletlen változók (kulcsok) előállítására.

- A titkos kulcs az aktuális csatorna statisztikák (Received Signal Strength (RSS), Channel State Information (CSI), Channel Phase (CP)) alapján generálható.

- Erős védelem, mivel csak a két félnél (Alice és Bob) azonos a csatorna.
- A támadó (Eve) más helyen tartózkodik, így másik csatornát lát – mivel a rádiós tér lokális!





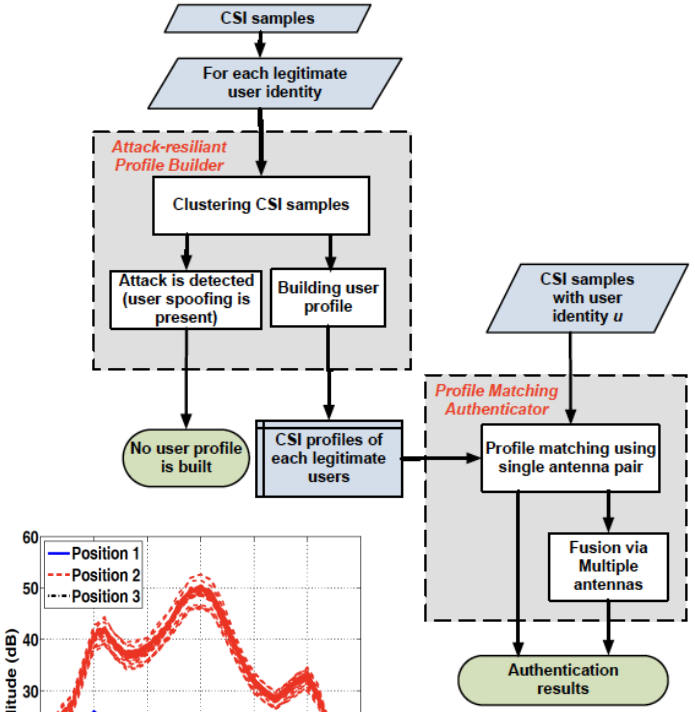
forrás: https://doi.org/10.1016/j.jisa.2024.103779

Példák: Csatorna alapú hitelesítés

- A két fél közötti csatorna jellemzőinek (fázis, amplitúdó, RSSI, CIR) gyors tesztelésén alapulnak.
- A mért paraméterek hash-elésével döntik el a hitelességet.

- Előny: nincs szükség előzetesen titkos kulcsra, frissíthető, gyors.

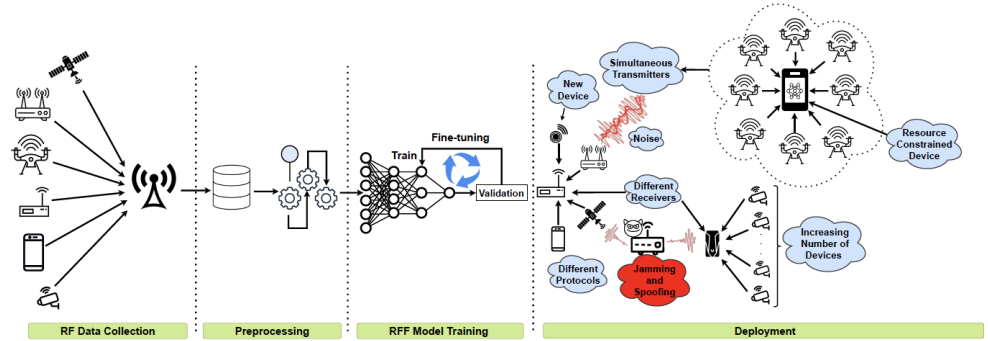
- Hátrány: a csatorna lassú változása / ismétlődése sebezhetőséget okozhat.

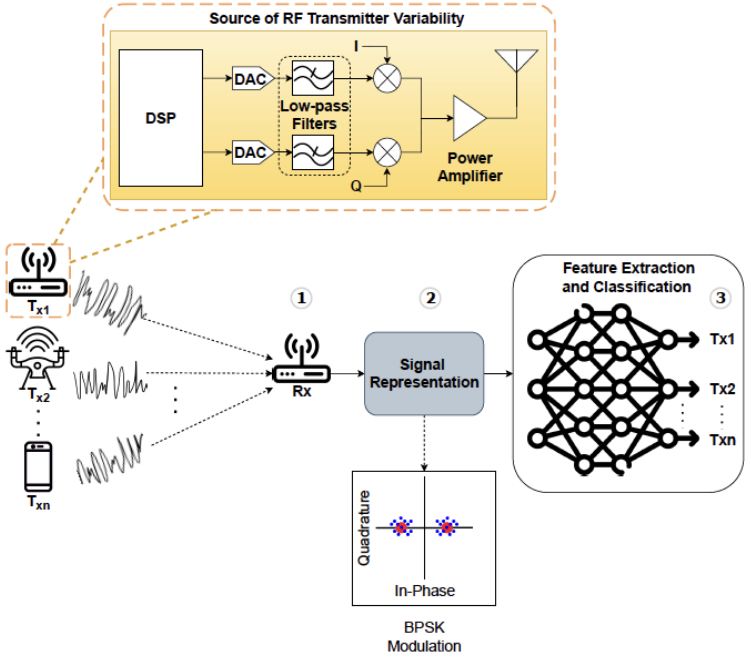


forrás: https://doi.org/10.1145/2590296.2590321

Példák: RF és device fingerprinting technikák

- Az adóegységek gyártásakor mikrohibák, minimális hardver hibák keletkeznek, melyek sajátos spektrum- vagy hullámformát hagynak az adásban.
- A vevő egyértelműen beazonosíthatja a hardvert.
- Drónok, IoT és okos járművek.





forrás: https://arxiv.org/pdf/2310.16406v2

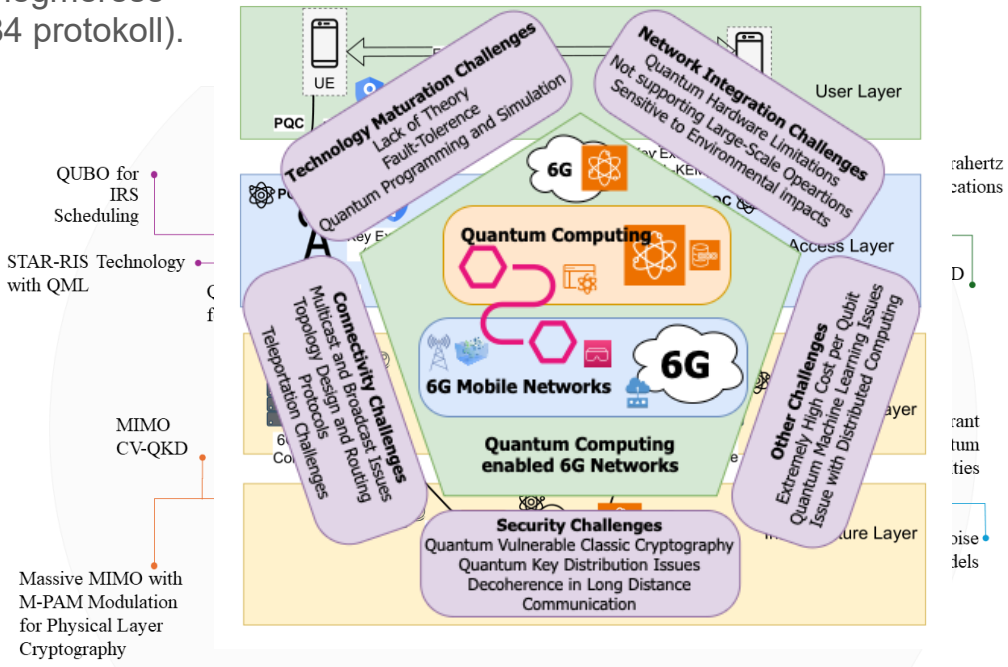
Példák: Kvantum alapú kulcselosztás (QKD)

- A kvantummechanika törvényein alapul, feltörhetetlen.
- A lehallgatás azonnal észlelhető – a qbitek megmérése megváltoztatja a kvantumállapotot (pl. a BB84 protokoll).

- 6G integráció:
  - a 6G maghálózatokban,
  - Free Space csatornákon, vagy akár
  - műholdas SatQKD rendszerekben.

- Előnyök:
  - Feltörhetetlen biztonság
  - Azonnali lehallgatás-észlelés
  - Harvest now, decrypt later elleni védelem

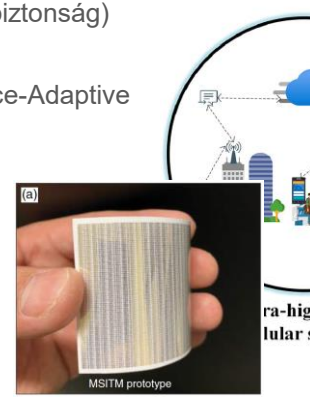
- Kihívások:
  - Kulcssebesség és skálázhatóság
  - Hardver és infrastruktúra
  - Integráció: QKD + PQC és hibrid kriptográfiai rendszerek.

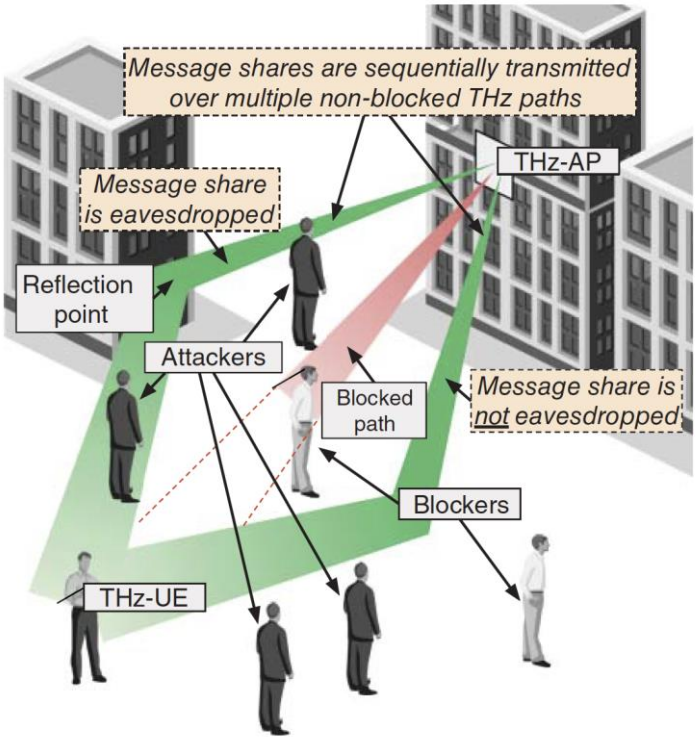


forrás: https://arxiv.org/html/2504.17133v1

Terahertz csatornák speciális biztonsági lehetőségei

- 6G-ben a terahertzes csatornák (0,1–10 THz) különleges biztonsági lehetőségeket biztosítanak
  - fizikai réteg sajátosságok
  - extrém irányíthatóság
  - nagy sávszélesség
  - speciális terjedési jellemzők
- Előnyök:
  - Magas irányíthatóság és szűk nyaláb („pencil-beam”)
  - Multipath és blokkolási védelem (multimodális biztonság)
  - Beltérre szabott biztonság
  - Absorpciós csúcsok/adaptív moduláció (Distance-Adaptive Absorption Peak Modulation)
- Speciális technikák:
  - Metasurface/IRS (intelligens felületek)
  - Physical Layer Key Generation
  - Adaptive beam hopping/wavefront hopping
  - Anti-jamming



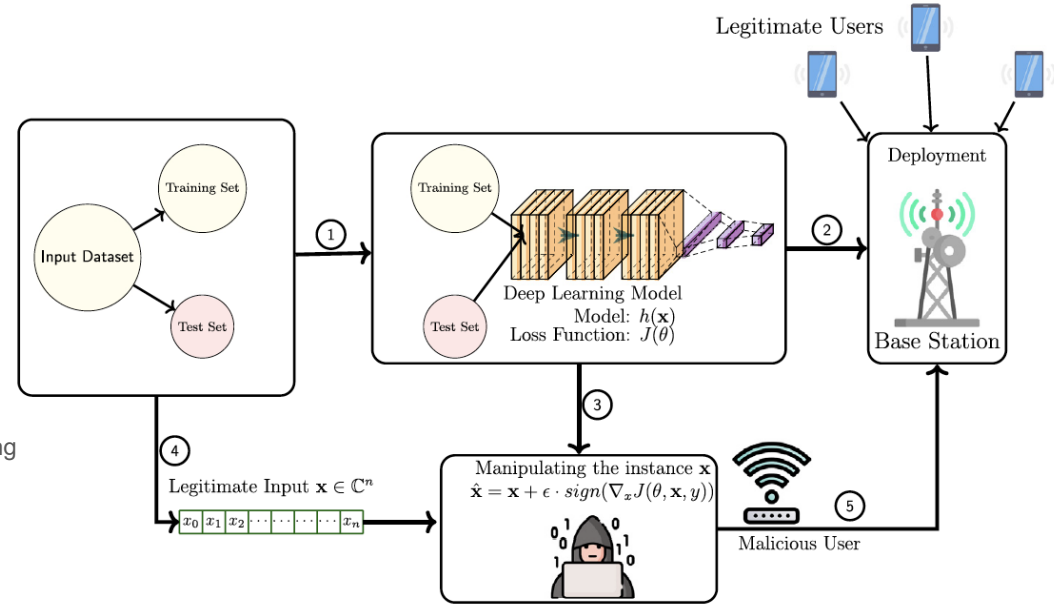


forrás: Physical Layer Security for Terahertz Communications in Massive IoT

forrás: https://doi.org/10.1016/j.fmre.2024.09.012

AI-alapú támadások és védekezési megoldások

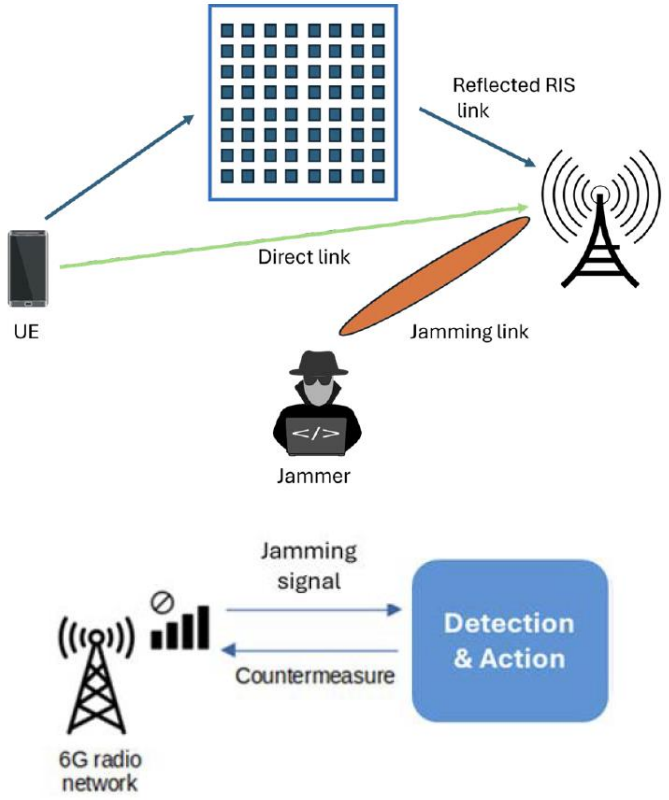
- Központi szerep az AI alapú biztonsági megoldásoknak
  - proaktív, adaptív és valós idejű fenyegetésészlelés, automatikus válaszadás
- Gépi tanulás és deep learning modellek (pl. Deep Neural Network) elemzik a hálózati forgalmat
  - hibák, támadások vagy anomáliák detektálása
- AI alapú PHY hitelesítés
  - RF fingerprinting, CSI vagy más hardveres/spektrális jellemzők automatikus felismerése
  - Adaptív jamming elleni védelem reinforcement learning megoldásokkal
- AI-alapú digitális iker (digital twin)
  - Az AI folyamatosan szimulálja és elemzi a valós infrastruktúra állapotát,
  - védelmi szcenáriókat tesztel



forrás: https://doi.org/10.1016/j.phycom.2022.101626

Adaptív jamming elleni védelem

- Mozgó eszközök azonosításához, védelméhez használható adaptív technikák:
  - spektrum szétválasztása
  - dinamikus irányított antenna vezérlés
  - Doppler-jelenség felhasználása
- Ezen technológiák csak 6G-nél, előre programozott, AI által menedzselt rendszerekben működnek igazán.
- Főként gépi tanuláson, játékelméleten, intelligens hullámformázáson és Reconfigurable Intelligent Surface (RIS) technológiákon alapulnak.



forrás: https://6g-ia.eu/wp-content/uploads/2025/01/wg_sec_position_paper-23.pdf

A fizikai réteg biztonsági megoldások összehasonlítása

Megoldás	Előny	Korlát	Tipikus alkalmazás
Channel fingerprint	Nincs szükség kulcsra	Ismétlődő csatornák	IoT, szenzorhálózatok
RF fingerprint	Hardveren alapul	Eszközcsere	Jármű, drón azonosítás
QKD	Kvantumbiztos	Költséges	Magas biztonságú linkek
AI anomaly detection	Gyors, adaptív	Túltréning	Valós idejű védelem
Adaptív beamforming	Infrastruktúra nélkül	Sávkorlátos	THz ultranagy sűrűség

Összegzés

- A 6G fizikai réteg biztonságának fő megoldása: csatorna-alapú hitelesítés, RF ujjlenyomat, QKD, adaptív AI-alapú támadásvédelem.
- A folyamatosan változó rádiós környezet új támadási és védekezési technikákat igényel.
- Jövő: autonóm, adaptív, prediktív biztonsági rendszerek már a fizikai rétegben is.

Köszönöm a figyelmet!