Az 5G rádiós interfész biztonságával kapcsolatos kutatás bemutatása INFOLAB

Németh Attila – Óbudai Egyetem

InfoLab Projekt

Az Infokommunikációs és Információtechnológiai Nemzeti Laboratórium (InfoLab) kettős célt tűzött ki maga elé: kutatásainak támogatnia kell a feltörekvő technológiák biztonságos bevezetését és alkalmazását; valamint az államigazgatás digitális átalakulását.

NBSZ Alprojekt

Nemzetbiztonsági és kiberbiztonsági célú kutatási-fejlesztési célterületek

- 5G RI protokoll és sérülékenység vizsgálata
- Valós idejű sérülékenység információ management
- Internet Survey Hungary
- IoT eszközök biztonsági minősítése

IdomSoft Alprojekt

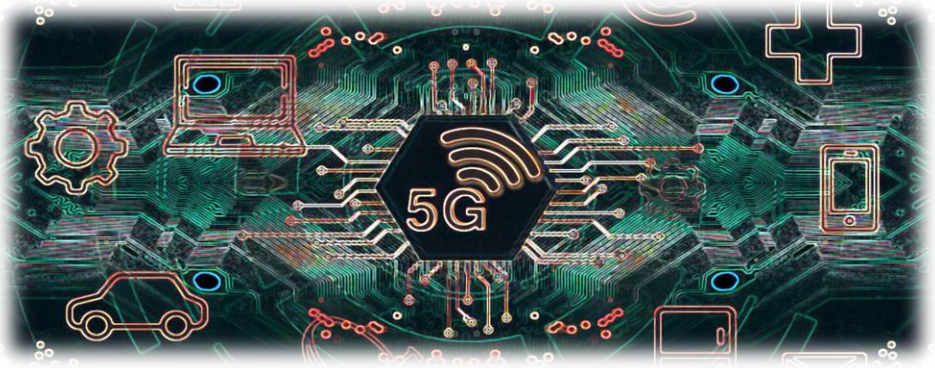
E-közigazgatási, rendvédelmi és rendészeti kutatás-fejlesztési célterületek

- a) Az alapnyilvántartások és a nemzeti adatvagyon nyilvántartásokhoz kapcsolódó szakrendszerek szemantikai interoperabilitásának kapcsolódása MI technológiákhoz;
  b) A közigazgatási szakrendszerek elektronikus (automatikus) együttműködését megteremtő köztesréteg kapcsolódása az adaptív megoldásokhoz
  c)Az ügyintézési eljárások formális leírásához és gépi reprezentáció megvalósításához szükséges K+F
- A mesterséges intelligencia alkalmazásának kutatása;
  MI technológián alapuló fejlesztési integrálási pontok
- A nemzeti adatvagyon védelméhez szükséges K+F;
  A nemzeti adatvagyon nyilvántartások és a hozzá kapcsolódó szakrendszerek biztonságos működtetéséhez szükséges architekturális elemek elkészítése, integrálása
- Biztonságos Digitális Társadalom Innovációs Klaszter

InfoLab – NBSZ alprojekt kutatási tevékenysége

❑ 5G

- RI protokoll vizsgálata
- RI sérülékenység vizsgálata



❑ Kibervédelmi kutatások

- Valós idejű sérülékenység információ management
- Internet Survey Hungary
- IoT eszközök biztonsági minősítése

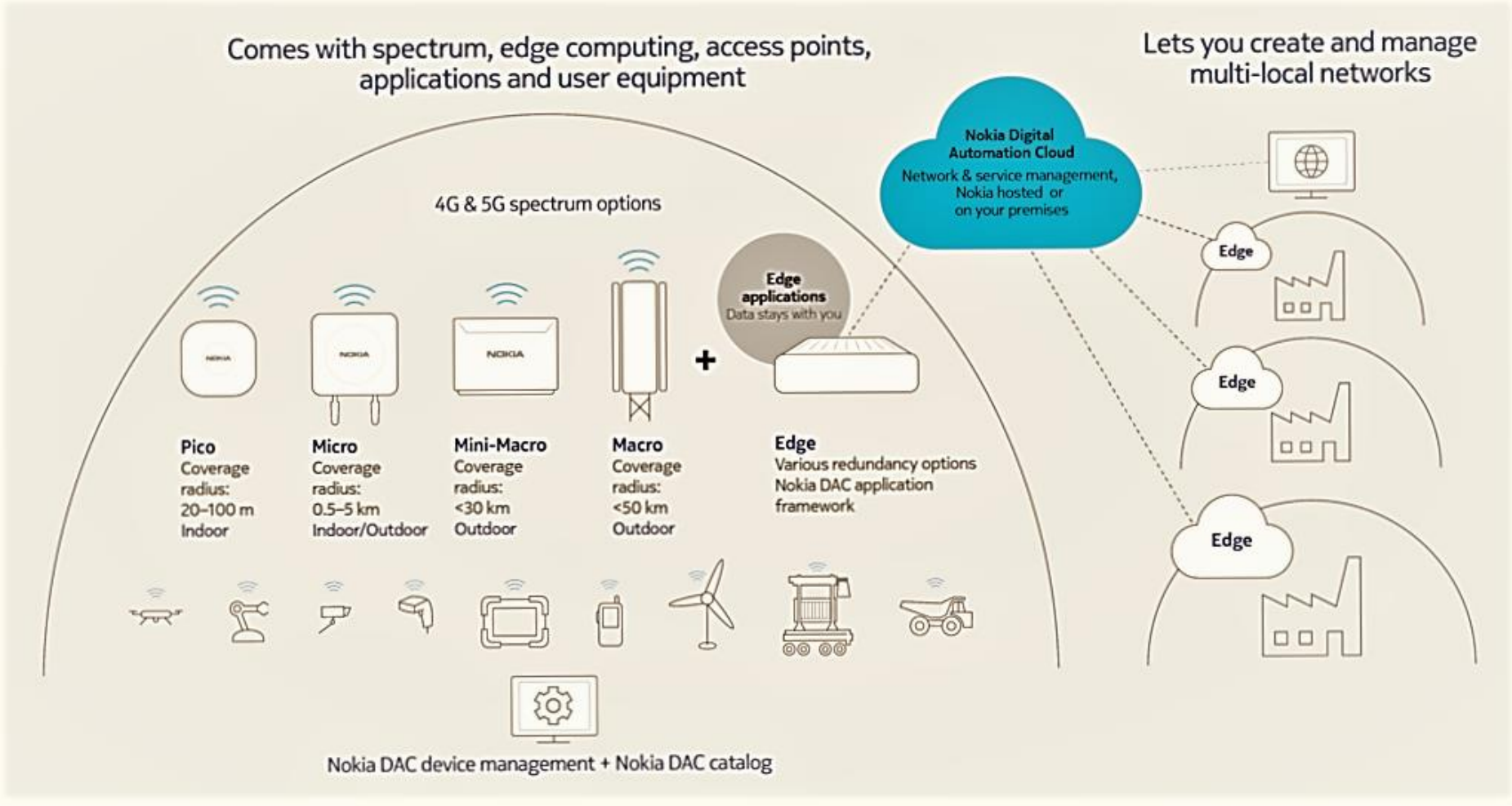
INFOKOMMUNIKÁCIÓS ÉS INFORMÁCIÓTECHNOLÓGIAI
Nemzeti Laboratórium

5G kutatási célok a biztonság fokozása érdekében

- 5G, 5G+, valamint a fejlettebb (6G, MI) hálózatokon alkalmazott rádiós protokollok ismeretének megszerzése,
- felhasználókhoz/mobil eszközökhöz köthető (technikai) azonosítók,
- átvitelre kerülő felhasználói, előfizető kommunikáció védelmi megoldásai,
- illetéktelen hozzáférés elleni védelem érdekében adatok rádiós interfészen keresztül történő megismerhetősége,
- gyakorlati mérések elvégzése: ismeretek felhasználása valós tesztkörnyezetben, spektrumvizsgálat, modulációelemzés, 5G NR jelzésrendszer/meta-adatok,
- rádiós zavarhatóság/zavartatás biztonsági kérdései.

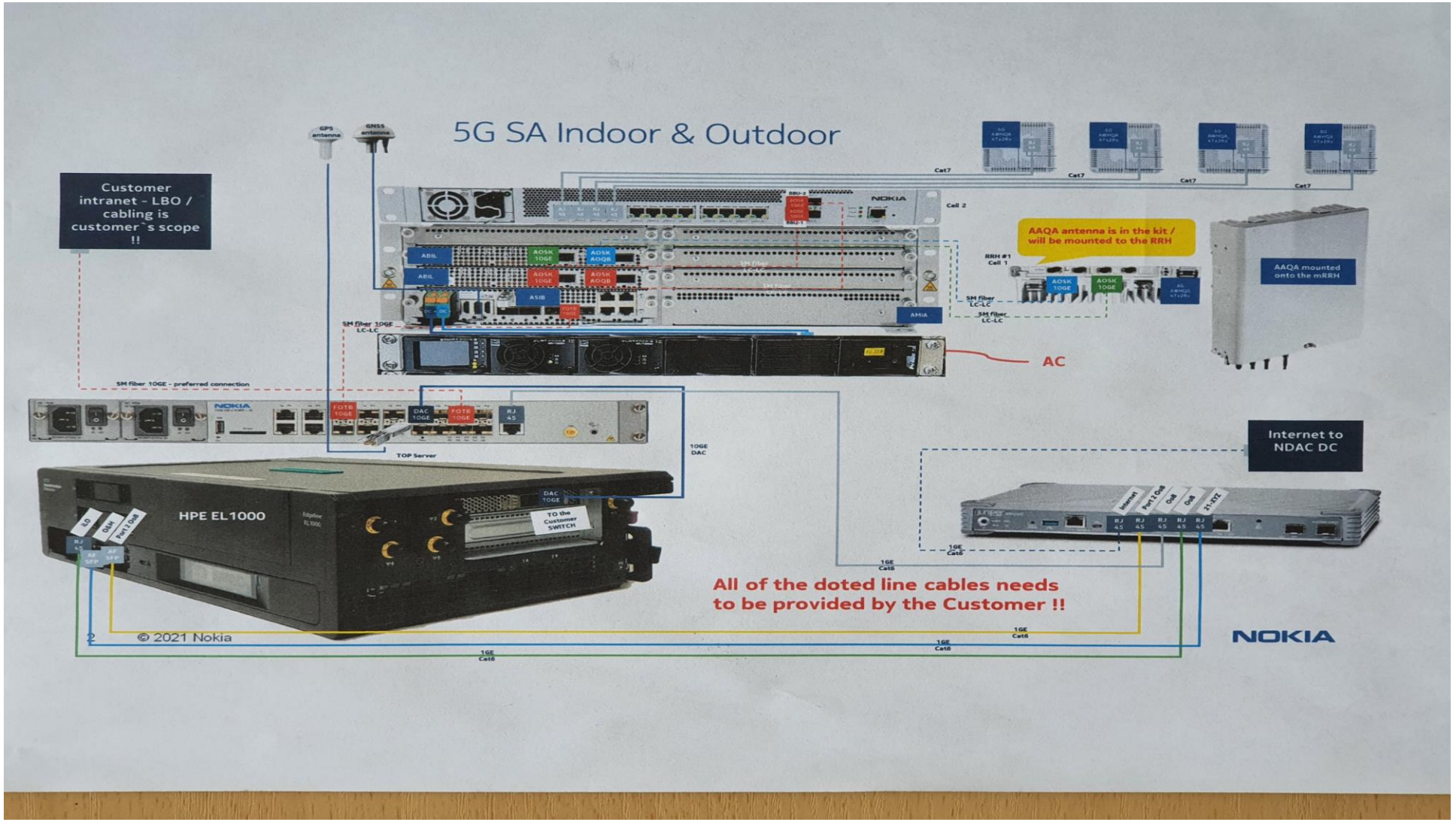
5G kutatás - infrastruktúra

NOKIA NDAC – 5G Stand Alone teszt hálózat



VODAFONE működési frekvencia – 3.5 GHz/40MHz sáv

Teszthálózat – SDR eszközök



5G teszt labor – Óbudai Egyetem - KVK

INFOKOMMUNIKÁCIÓS ÉS
INFORMÁCIÓTECHNOLÓGIAI
Nemzeti Laboratórium

5G szinkronizáció sérülékenység

Cél: szinkronizáció, mint sebezhetőségi pont behatárolás

- **Kitűzött feladatok:**
  - ❑ Szinkron források lekapcsolás – hatásvizsgálat;
  - ❑ Szinkron forrás zavartatás – zavartatás vizsgálat (hatásosság bizonyítás, vagy elvetés);
  - ❑ Zavaró eszköz (SDR alapú) létrehozása.
- **Elvárt eredménytermék:**
  - ❑ Hálózat stabilitás / instabilitás kimutatása;
  - ❑ Zavarhatóság definiálása.
- **Eredmények hasznosulása:**
  - Szinkron sérülékenység definiálás;
  - Hálózat tervezők számára fontos információk a szinkron redundancia kialakítására, szinkron források elhelyezésére.

5G szinkronizáció sérülékenység

Eredmények:

- Bizonyítást nyert, hogy az 5G hálózatok „Achilles ín”-e a szinkronizáció.
- A gyakorlati kísérletek alátámasztották feltételezéseinket.
- Eredmények alapján gyakorlati útmutatások fogalmazhatók meg az 5G hálózattervezők részére.

Eredményeinket publikáltuk:

SISY 2022

IEEE 20th Jubilee International Symposium on Intelligent Systems and Informatics

Tibor Wührl – Péter János Varga
Sándor Gyányi – Márk Baross – Attila Németh:

5G RAN synchronization vulnerability

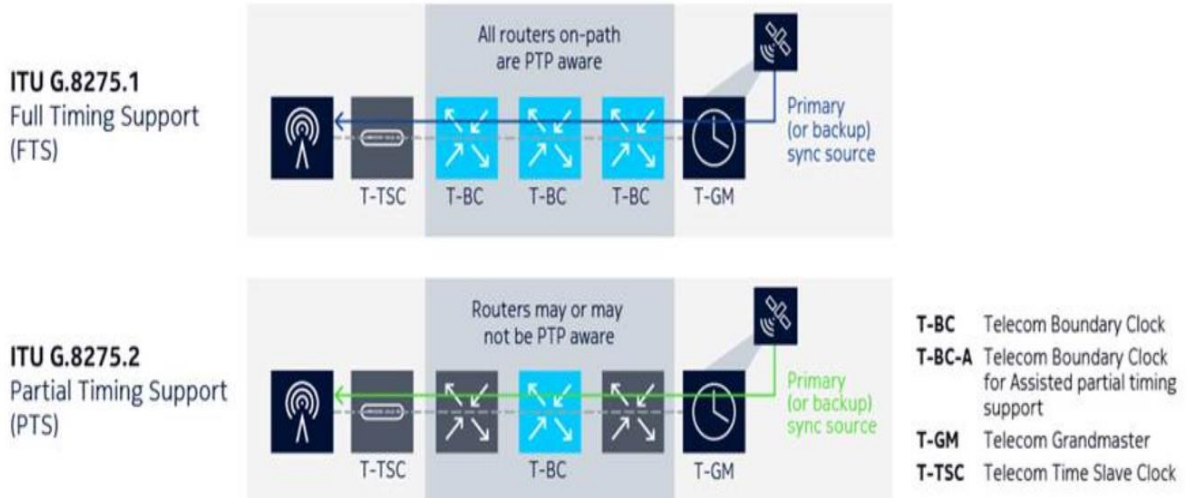
5G szinkronizáció sérülékenység hasznosulása

A NOKIA blog is foglalkozott a szinkronizáció problémájával.*

Using the packet transport network as a backup synchronization source

Fortunately, packet transport networks that provide connectivity to cell sites can also distribute highly accurate synchronization data. With 5G gNBs requiring both frequency and time/phase synchronization, the transport nodes can provide synchronization using Synchronous Ethernet (SyncE) and the IEEE 1588v2 Precision Time Protocol (PTP). The PTP can work with various timing profiles (see Figure 1).

Figure 1. Timing profiles



*forrás: https://www.nokia.com/blog/timing-and-synchronization-options-to-support-5g/

5G RAN - SOC


Log Collection
Reporting
Aggregation
Correlation
Security
Operation
Center (SOC)
SIEM
Research &
Development
Ticketing
Threat
Intelligence
Knowledge
Base

5G RAN sérülékenység vizsgálat – SOC vonatkozások

SOC szimulációs környezet fejlesztése, 5G implementálása:

- központi napló- és forgalomelemző:
  - naplóadatok integrálása,
  - forgalmi adatok gyűjtése és elemzése
- fizikai SDR eszközök integrálása

  → SIEM használati esetek tervezését és megvalósítását támogatják,

  → előkészítik a lehetőségét a neurális hálóval támogatott behatolás detektálás és felhasználó/végpont profilozását.
- továbbá vizsgálatok:

  támadási gráfok 5G hálózatokban történő alkalmazhatósága: sérülékenységvizsgálat, kockázat elemezés vagy behatolás detektálás

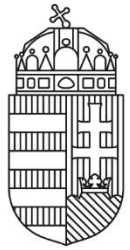
Kutatási eredmények:

❑ RI sérülékenység vizsgálat:

- „5G registration tracking based on logdata” (ICCC 2022)
- „Security threats based on critical database system privileges” (ICCC 2022)

❑ RI protokoll vizsgálat:

„Jamming Attacks in 5G NR FR1” (CANDO EPE 2022),
„5G RAN synchronization vulnerability” (SYSY 2022),
„Enhancing Trust in 5G” (INNES 2022),
„The Mobile Ecosystem, 5G and NESAS” (ICCC 2022).



NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

A bemutatásra került kutatást, a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatta az Infokommunikációs és Információtechnológiai Nemzeti Laboratórium keretében.

INFOKOMMUNIKÁCIÓS ÉS
INFORMÁCIÓTECHNOLÓGIAI
Nemzeti Laboratórium

Köszönjük a figyelmet!