Új algoritmusok és kódolási eljárások alkalmazása a mobil hírközlésben és informatikában

A mobil kommunikáció és informatika korunk egyik legdinamikusabban fejlődő mérnöki szakterülete. A világon kutatócsoportok egész serege foglalkozik a téma művelésével, nap mint nap új elméleti eredmények látnak napvilágot, új technológiai megoldások és új szolgáltatások születnek. Az elmúlt évtizedben a mobil kommunikációs rendszerek több korszakon mentek keresztül. Ma a második generációs mobil távközlési rendszereket használjuk (GSM, IS-95, DECT, TETRA), de a nemzetközi kutatások már a harmadik és negyedik generációs rendszerek elméleti és gyakorlati kérdéseivel foglalkoznak. Emellett a téma az EU fejlesztési programjaiban (Framework 5., 6.) és az USA tudományos kutatási támogatási rendszerében (NSF) is kiemelt szerepet kapott a mobil távközlési és informatikai rendszerekkel és szolgáltatásokkal kapcsolatos alapkutatások támogatása, mivel általánosan elfogadott az az állítás, hogy az Információs Társadalom technológiai infrastruktúrájának domináns eleme lesz a mobil hírközlési és informatikai hálózat.

A pályázat az átfogó cím mellett négy alapvető szakterületen fogalmazta meg kutatási célkitűzéseit. E kérdéskörök között is van néhány olyan, amely elméleti szempontból és a gyakorlati alkalmazások előkészítése oldaláról nézve is kiemelt jelentőségű. Ezek közé tartoznak azok a technológiák, algoritmusok és protokollok, amelyek a korszerű mobil rendszerekben a mobilitást támogatják és azok az informatikai biztonsági rendszerek, amelyek a megbízható és védett szolgáltatásokat lehetővé teszik. E témák nagy kihívást jelentenek nemcsak a mérnökök és technológusok számára, hanem sok új elméleti problémát vetnek fel, például a matematikai kutatás számára is. Nem véletlen, hogy kutatócsoportunk nem csak műszaki szakemberekből áll, hanem fontos szerepet kaptak benne elméleti és alkalmazott matematikusok is.

Az igen komplex kutatási területen kutatócsoportunk az alábbi aktuális résztémákban kívánt kutatási munkát végezni:

- **A mobil technológiák területén:**
  - A heterogén mobil hálózatok együttműködési problémái
    - Mobilitási problémák elemzése a különböző technológiák integrációja esetén
    - A megszakadás-mentes hívásátadás algoritmusainak fejlesztése, szimulációja és modellezése
    - Mikro-, makro- és hierarchikus mobilitás vizsgálata heterogén IP hálózatokban
    - Az átvitel minőségét (QoS) támogató eljárások vizsgálata valós idejű adatátvitel esetén heterogén mobil hálózatokban,
    - A mobilitás támogatása “otthoni” mobil hálózatokban, az “otthoni” mobil hálózatok architekturális kérdései
    - A heterogén mobil hálózatok együttműködését támogató hálózatmenedzselési módszerek vizsgálata
  - A mobil Internet Protokoll alkalmazásával kapcsolatos vizsgálatok
    - Teljesen integrált IP alapú mobil hálózatok vizsgálata
    - Mobil IP feletti adatátviteli eljárások minőségének az elemzése

- Többfelhasználós detekciós módszerek a kódosztásos többszörös hozzáféréses mobil rendszerekben
  - A megvalósítható többfelhasználós detekciós eljárások vizsgálata
  - Komplex többfelhasználós detekciós eljárások fejlesztése
- A heterogén mobil hálózatok forgalmi modellezése
  - A hagyományos forgalmi modellek módosított változatainak a vizsgálata mobil hálózatokban
  - A mobil hálózatok támogatására szolgáló egyéb algoritmusok vizsgálata

➢ **A hálózatok, rendszerek és szolgáltatások biztonsága területén:**

- A mobil informatikai és távközlési hálózatok, rendszerek és szolgáltatások biztonsági kérdései
  - Adatvédelemi és adatbiztonsági eljárások fejlesztése és elemzése mobil informatikai és távközlési hálózatokban, rendszerekben és szolgáltatásokban
  - Az elektronikus kereskedelem biztonsági problémái (web biztonság, fizető protokollok, kulcskezelés, információ védelem, stb.)

➢ **A mobil hálózatokkal, rendszerekkel és szolgáltatásokkal kapcsolatos algoritmusok és kódolási eljárások területén:**

- Útkeresési és csatornakijelölési algoritmusok fejlesztése és vizsgálata mobil hálózatok számára
  - Gráfelméleti alkalmazások, kombinatorikus optimalizálási módszerek
  - Útkeresési és közeghozzáférési eljárások ad hoc mobil hálózatokban
- A mobilitást támogató diszkrét algoritmusok, kódolási eljárások mobil hálózatokban
  - A mobilitás diszkrét algoritmusai
  - Kódolás mobil rendszerek számára

A tudományos iskolában közel húsz doktorandusz dolgozott. Többen közülük a kutatási támogatás ideje alatt megvédték, illetve már lényegében befejezték PhD disszertációjukat, mások – a doktori folyamat elkezdésének időpontjától függően – előrehaladtak a kutatási terület művelésében. Az alábbiakban a tervnek megfelelő sorrendben adjuk meg a kutatásban elért eredményeket

A kutatás eredményei:

➢ **A mobil technológiák területén:**

- A heterogén mobil hálózatok együttműködési problémái területén

Konkrét eredmények:

- 3G- és WLAN hálózatok együttműködése,
- Vezeték nélküli számítógép hálózatok analízise,
- Az LTRACK – új mobilitás menedzsment algoritmus analízise és szimulációs vizsgálata a mobilitás és a hívásátadás szempontjából, az algoritmusok összehasonlító elemzése,
- Az LTRACK rendszer paramétereinek hatáselemzése, méretezési eljárás kidolgozása, új mobilitás modell kidolgozása, Markovi modellek alkalmazása,
- A klasszikus mozgásmodellek analitikus vizsgálata (hány felhasználó lesz egy adott cellában a (t+1)-edik diszkrét időtartamban? Egy felhasználó

mekkora valószínűséggel jut el egy *i*-edik cellából egy *j*-edik cellába egy diszkrét *t* időtartamon időn belül? *N* felhasználó esetén, milyen gyakorisággal történik cellaváltás a rendszerben? Hatékony hálózatméretezési eljárások kidolgozása,
  - Az IPv6 Anycast címeinek felhasználása a mikromobilitás támogatására, a rendszer tesztelése. Az új eljárás analitikus és szimulációs elemzése,
  - A mobil ügynök technológia alkalmazása a nagyméretű hálózatok menedzselésére, az előfizetők számára költséghatékony szolgáltató választásra, ad hoc hálózatok menedzselésére. A mobil ügynök rendszer új algoritmusainak a kidolgozása, ezek valószínűségi modellezése és hatékonyságvizsgálata,
  - A heterogén mobil hálózatok együttműködését támogató hálózatmenedzselési módszerek vizsgálata,
- A mobil Internet Protokoll alkalmazásával kapcsolatos vizsgálatok

Konkrét eredmények:

  - Multimédia átvitel mobil hálózatokban,
  - Számlázási feladatok a Next Generation mobile hálózatokban,
  - Web2Wap az intelligens konverter eszköz az on-line HTML-től a WML-ig,
  - Heterogén rendszerek számlázási kérdései, ezen belül a harmadik generációs mobil hálózatok számlázási algoritmusainak kidolgozása, a valós idejű számlázás elméleti és gyakorlati megvalósításának vizsgálata. Olyan számlázási architektúrára, mely alkalmas az online és offline számlázás együttes kezelésére és figyelembe veszi a különböző szolgáltatások minőségét és speciális igényeit.
  - Mobil IP hálózatok modellezése a fizikai modell, az analitikus modell [HMIP] és a szimulációs modell [MMSIM] vizsgálata.
- Többfelhasználós detekciós módszerek a kódosztásos többszörös hozzáféréses mobil rendszerekben

Konkrét eredmények:

  - Quantum Computing and Communications An Engineering Approach,
  - Kvantumszámítási alapú valószínűségi sűrűségfüggvény becslés,
  - Maximum Likelihood halmaz szeparáció,
  - Multiple-Access Capability of Synchronous of FHSS Wireless Networks: An Analysis of the Effects of the Spacing between Hopping Carriers,
  - A bináris és kvaternális PSK rendszerek pontos hibaanalízise diverziti és azonos frekvenciás interferencia esetén,
  - Accurate Evaluation of Packet Error Probabilities Considering Bit-to-Bit Error Dependence,
  - Általános hibaanalízis interferencia-korlátozott rádiós hálózatokban,
  - Új visszacsatolt neurális hálózatokon alapuló többfelhasználós vevők kidolgozása és hatékonyságvizsgálata,
  - A közös forrás- és csatornakódolás/dekódolás (Joint Source and Channel Coding/Decoding – JSCC/D) vizsgálata, és illesztése az UMTS rendszerbe.

- A kvantumszámítási eljáráson alapuló több felhasználós vevők kialakítása és analízise. A Grover-keresést alkalmazása optimális vevőben. A valószínűségi eloszlásfüggvény becslése kvantumszámítási algoritmussal,
- A független komponens analízis (ICA) és a vak forrás szeparáció (BSS) felhasználása az interferenciák elnyomására,
- A vak forrás szeparációs kutatás alkalmazása a vak csatornabecslésre és csatornakiegyenlítésre. Az úgynevezett semi-blind módszerek vizsgálata,
- A több bemenetű több kimenetű (MIMO) rendszerek analízise. Az ICA és BSS algoritmusok adaptív MIMO rendszerekben történő alkalmazhatósági analízise.

- A heterogén mobil hálózatok forgalmi modellezése

Konkrét eredmények:

- Modified Radial Basis Network Based Blind Channel Estimation,
- Multiumedia Transmission over Mobile Networks,
- Számlázás heterogén mobil hálózatokban,
- A rádiós hálózatok új tervezési módszerei a forgalmi adatok alapján, a Phase Type eloszlások felhasználása a méretezésben, a kapacitások dimenzionálása,
- Hívásengedélyezési eljárások harmadik generációs mobil hálózatok számára.

➢ **A hálózatok, rendszerek és szolgáltatások biztonsága területén:**

- A mobil informatikai és távközlési hálózatok, rendszerek és szolgáltatások biztonsági kérdései

Konkrét eredmények:

- A Game Based Analysis of the Client Puzzle Approach to Defend Against DoS Attacks,
- Olcsó RFID eszközök egyszerű autentikációs protokolljai,
- Equilibrium Analysis of Packet Forwarding Strategies in Wireless Ad Hoc Networks -- the Static, A fast APRIORI implementation,
- Rosszhiszemű terminálokról küldött autentikus üzenetek kezelése,
- Igazolható biztonságú on-demand forráskeresés mobile ad hoc hálózatokban,
- Igazolható biztonság ad hoc útkeresési eljárásokhoz,
- Komponensek a spam-ok és vírusok elleni védelemhez,
- Csomóponti kooperáció hibrid ad hoc hálózatokban,
- Standards for Product Security Assessment,
- A framework for the revocation of unintended digital signatures initiated by malicious terminals,
- Az e-mail vírusok és kéretlen reklámlevelek elleni eljárások kidolgozása, a forgalmi mérések segítségével DoS és víruskitörési támadások ellen védekezhetünk statisztikai módszerekkel. Játékelméleti módszerekkel történő kezelés.
- Az „Trap E-mail Address” módszer kidolgozása és éles tesztelése. Új rendszerelméleti megoldások kialakítása.

- **A mobil hálózatokkal, rendszerekkel és szolgáltatásokkal kapcsolatos algoritmusok és kódolási eljárások területén:**
  - Útkeresési és csatornakijelölési algoritmusok fejlesztése és vizsgálata mobil hálózatok számára
  - Útkeresési és közeghozzáférési eljárások ad hoc mobil hálózatokban A mobilitást támogató diszkrét algoritmusok, kódolási eljárások mobil hálózatokban

  Konkrét eredmények:
  - Hash-fák és szófák az adatbányászatban,
  - Automatic Discovery of Locally Frequent Itemsets in the Presence of Highly Frequent Itemsets,
  - Meglepő eredmények a Trie-based FIM algoritmusokkal kapcsolatban,
  - List edge multicoloring in graphs with few cycles,
  - Gráf szinezési módszerek és azok alkalmazása az ütemezésben,
  - A multiszinezésű fák csúcsainak minimális összege,
  - Paraméteres gráf szeparálási problémák,
  - Parameterized coloring problems on chordal graphs,
  - Parameterized complexity of constraint satisfaction problems,
  - Maps of matroids with applications,
  - Improving size-bounds for subcases of square-shaped switchbox routing,
  - On the complexity of the channel routing problem in the dogleg-free multilayer Manhattan model,
  - A kétrétegű Manhattan csatorna keresés egy új algoritmusa,
  - Szignature kódolás és információátvitel többszörös hozzáférésű összeadó csatornában,
  - Trie: egy alternatív adatstruktúra adatbányászati algoritmusokhoz,
  - Filtering False Alarms: an Approach Based on Episode Mining,
  - List edge multicoloring in bounded cyclicity graphs,
    Minimum sum multicoloring on the edges of trees,
  - Maps of matroids with applications,
  - Benchmarking Frequent Itemset Mining Algorithms: from Measurement to Analysis,
  - Többszörös hozzáférésű összeadó csatorna kódolása,
  - One-dimensional synthesis of graphs as tensegrity frameworks,
  - The evolution of an idea – Gallai/’s algorithm,
  - On the generalization of the matroid parity problem,
  - Gráfszínezési problémák, illetve egyéb algoritmikus problémák vizsgálata paraméteres bonyolultságelméleti szempontból,
  - Hatékonyan megoldható feladatok és a nehéz feladatok közötti határvonal felderítése, például a listás élmultiszínezés polinom időben megoldható esetei, a színezésbővítés és az ún. chromatic strength problémák élesebb bonyolultsági eredményei,
  - Paraméteres algoritmusok, illetve a W[1]-teljesség eszköztárának alkalmazása nehézségi eredményeket bizonyítására,

- Gráfelméleti problémák körében a szeparálási feladat különböző változatainak vizsgálata, illetve a bizonyos speciális gráfosztályok színezése. Hatékonyság közelítő algoritmusok létezésének elemzése,
- A gráfelmélet területén megfogalmazódó NP-teljes problémák vizsgálata. Elsősorban a különböző költségfüggvények tekintetében az optimálishoz garantáltan közel álló költségű feszítőfák keresése,
- A gráfelméleti feladatok alkalmazása a modern távközlési hálózatok tervezésére,
- Approximációs algoritmusok kidolgozása, a matematikailag nem igazolt heurisztikák gyakorlati viselkedésének lemérése, illetve a fontosabb gráfparaméterekkel (pl. tree-width, átmérő, út-partíciós szám, stb.) való kapcsolat feltárása,
- Weboldakat kereső algoritmusok, illetve tematizáló programok spektrális módszereket alkalmazó családjának vizsgálata mátrixok szinguláris értékek szerinti felbontásával (SVD),
- A weboldalak rangsorolására szolgáló Page Rank algoritmus módosításával a linkgyűjteményeket rangsoroló eljárás tervezése
- Új jól skálázható algoritmus a weboldalak hasonlóságát mérő SimRank és a weboldalak érdekességét illetve népszerűségét mutató Personalized PageRank értékek kiszámítására,
- Véletlen mintavételezésen alapuló Monte-Carlo módszerrel alkalmazása a fenti feladat megoldására,
- Kódkorlátok vizsgálata az identifikációs probléma esetén, a Lindström konstrukció egyszerűsítése a többszörös hozzáférésű összeadó csatorna identifikációs problémájára,
- Identifikáció és dekódolás együttes problémája, a kapacitáskorlátot megközelítő kódkonstrukciók keresése, populációméret becslése,
- Ad-hoc hálózatok alapvető problémái, kapacitáskorlátok és konnektivitás vizsgálata, a többszörös hozzáférésű csatornák kódolási korlátainak és konstrukcióinak vizsgálata ad-hoc környezetben, ad-hoc hálózatok problémáinak elemzésére,
- Egy új (binomiális) felhasználói aktivitási modell kidolgozása, mellyel az eddig alkalmazott modellhez képest lényegesen kisebb kódszóhosszal is kis hibavalószínűségű, azaz megbízható kommunikáció biztosítható a felhasználók között a VAGY csatornán,
- A VAGY csatornán alkalmazott Kautz–Singleton kódkonstrukció hibavalószínűségének pontos kiszámítása,
- A többszörös hozzáférésű ütközéses csatornán a Bassalygo és Pinsker által vizsgált visszacsatolás nélküli bináris csomagkommunikáció általánosítása nem bináris csomagok illetve aszinkron hozzáférés esetére,
- A gyors frekvenciaugratásos csatornán az aszinkron jelzéskódolást elemzése.