Előszó

szabo@hit.bme.hu

Jelen számunk válogatás az utóbbi időszakban a lap számára beküldött és részben bírált cikkekből. Amint az az alábbi rövid bemutatásokból látszik, a cikkek témái széles spektrumot ölelnek fel. Ebben a számunkban egy új törekvés első lépése is látszik: szeretnék rendszeresen bemutatni a hazai kutatási-fejlesztési projektek eredményeit, elsőként most az Aitia International Zrt. és a BME Távközlési és Médiainformatikai Tanszék munkatársai által kifejlesztett érdekes rendszert.

Nagysebességű TCP-protokollok együttműködésének modellezésével foglalkozik *Simon Boglárka, Sonkoly Balázs és Molnár Sándor* cikke. A hagyományos TCP torlódásvezérlésében jelentkező problémák miatt nagysebességű és nagy kiterjedésű hálózati környezethez a közelmúltban több új, nagysebességű TCP verziót fejlesztettek ki, mint például a HighSpeed TCP és a Scalable TCP. A cikkben szabályozástechnikai modellezés alapú eredményeket ismertetnek a szerzők.

A vezetéknélküli hálózati végpontok mozgása mellett bizonyos esetekben egy alhálózat is változtathatja a helyét, ennek tipikus példája a járműveken belüli, együtt mozgó hálózatrész (mozgó hálózat). Az IETF Network Mobility (hálózat-mobilitás) csoportja a Mobil IP-hez hasonlóan kezeli ezt a kérdést, amely azonban a mozgó hálózatból fakadóan összetettebb probléma, mint az önálló végpontok mobilitása. *Kanizsai Zoltán, Rózsás Balázs és Imre Sándor* cikkükben a mozgó hálózatok mobilitás-támogatásával kapcsolatos eredményeket tekintik át a Mobil IP-ből kiindulva.

Perényi Marcell, Soproni Péter és Cinkler Tibor dinamikusan változó multicast fákkal foglalkoznak kétrétegű optikai hálózatokban. A levél-csomópontok állandó váltakozásával a fa egyre távolabb kerül az optimális topológiától, ezért sok hálózati erőforrás és költség takarítható meg a fa rendszeres újrakonfigurálásával, az optimális topológia visszaállításával. Vizsgálják eredményességét több dinamikus útvonalválasztó algoritmus és az újrakonfigurálási intervallum hosszának függvényében is.

A web már régóta felvet adatvédelmi kérdéseket a látogatók számára is: bizonyos szolgáltatók megfigyelik, követik a felhasználók tevékenységeit, adatbázist építenek ízlésvilágukról. Az anonim böngészők megoldást kínálnak a felhasználóknak; elrejtik őket a figyelő szemek elől. *Gulyás Gábor és Schulcz Róbert* bemutatnak néhány követésre használt módszert, illetve egy új, az anonimizáló szolgáltatásokra vonatkozó konstrukciós paradigmát, majd egy ez alapján értelmezett osztályozási rendszert is az anonim böngészők besorolásához.

A vezetéknélküli számítógéphálózatok használata közben a felhasználó szabadon helyet változtathat, ehhez kapcsolódóan alakult ki a felhasználó pozíciójától függő szolgáltatások köre. Ehhez szükségessé válik egy helymeghatározó rendszer kialakítása, amely beltérben is használható és megfelelő pontossággal rendelkezik ahhoz, hogy az arra épülő alkalmazások igényeit kiszolgálja. A *Németh László Harri, Kis Zoltán Lajos és Szabó Róbert* által kifejlesztett WLANpos megoldás célja egy Wi-Fi hálózat és egy szabványos Wi-Fi eszköz segítségével a vevő, azaz a felhasználó helyének lehető legpontosabb meghatározása volt, amely jobb az eddigi megoldásoknál, amelyek általában drágák, nagy számítási igénnyel rendelkeznek, vagy csak korlátozott térben alkalmazhatók.

Tartalomszolgáltatási alkalmazásoknál kulcskérdés a tartalom védelme, amelynek egyik módszere a vízjelezés (watermarking). *Oláh István* cikkében összefoglalja a videó-vízjelezés sajátosságait és bemutat egy olyan videó vízjelezési eljárást, ami ellenáll a H.264/AVC tömörítésnek és a legáltalánosabb jelfeldolgozási módosításoknak.

Napjaink kommunikációs hálózatainak gyakran nincs kiépített fix infrastruktúrája (pl. ad-hoc hálózatok, ambient intelligencia hálózatok vagy szenzorhálózatok). Ezek a hálózatok nagymértékű önállósággal, autonómiával rendelkeznek, s gyakran akár önző módon is viselkedhetnek. Hogy megszüntessük, illetve mérsékeljük az önző viselkedést a hálózatban, egy elosztott keretrendszer válik szükségessé, amely ösztönzi a résztvevőket a kommunikációra és az együttműködésre. A *Németh László Harri és Szabó Róbert* által vizsgált megoldás a hálózati topológia figyelembevételében különbözik az eddigiektől és egy újszerű megoldást mutat be erre a problémára.

Az API szintű támadások komoly veszélyt jelentenek a hardver biztonsági modulokra nézve, ezért fontos követelmény az API-ban rejlő biztonsági lyukak felfedezése és foltozása. Az API analízis egyik ígéretes iránya a formális verifikációs módszerek alkalmazása. *Buttyán Levente és Ta Vinh Thong* cikkükben ezt az irányt követik, s egy processz-algebra alapú API verifikációs módszert javasolnak, mely különösen alkalmasnak látszik a biztonsági API-k működésének formális leírására, a biztonsági követelmények precíz definiálására és a megfogalmazott követelmények teljesítésének ellenőrzésére.

Végül *Tatai Péter, Varga Pál és Marosi Gyula* mutatnak be egy távközlő hálózatok üzemi állapotainak folyamatos figyelésére, monitorozására alkalmas rendszert. A rendszer lehetővé teszi, hogy a hálózat forgalmi- és hívásstatisztikái alapján segítséget nyújtson a hálózat üzemeltetőjének a hálózat skálázható, dinamikus növelésére a szolgáltatások egyre bővülő választéka mellett.

Szabó Csaba Attila
főszerkesztő