Kooperációra ösztönző mechanizmusok többugrásos vezeték nélküli hálózatokban

BUTTYÁN LEVENTE, HOLCZER TAMÁS, SCHAFFER PÉTER

CrySyS Laboratórium (Laboratory of Cryptography and System Security)
BME Híradástechnikai Tanszék

{buttyan, holczer, schafi}@crysys.hu

Reviewed

Kulcsszavak: díjazás, cellás hálózat, számlaalapú ösztönzés, biztonság, kriptográfia

Cikkünkben bevezetjük a kooperációra való ösztönzés problémáját, ami tipikus problémaként jelentkezik a többugrásos vezeték nélküli hálózatokban. Röviden áttekintetjük a nem-kooperatív viselkedési fajtákat, és a kooperációra ösztönző mechanizmusok típusait. Végül összefoglaljuk két általunk javasolt ösztönző mechanizmus főbb elemeit, ötleteit.

1. Bevezetés

Az elmúlt évtizedben a számítógépes technológia hatalmas fejlődésen ment keresztül. Ez a fejlődés egyrészt a hagyományos számítógépek teljesítményének növekedésével járt, másrészt olyan új számítógépes eszközök és alkalmazások létrehozásának technikai feltételét teremtette meg, melyek jelentős mértékben megváltoztatják az informatika és a távközlés ma ismert arculatát. A számítógép, mint önálló eszköz mellett megjelentek és fokozatosan túlsúlyba kerülnek az „intelligens tárgyak", melyekben a számítógép beágyazott célhardver formájában van jelen. A modern telefonkészülékekben, autókban, háztartási eszközökben, bankkártyákban már ma is megtalálható a beágyazott számítógép, és ez a kör a jövőben még tovább bővül majd. A számítógépes technológia a szó szoros értelmében mindenhol jelen lesz majd *(ubiquitous computing)*.

A mindütt jelenlevő számítástechnika víziója nagy hatást gyakorol az informatika és a távközlés területén folyó kutatás egészére. Ennek kapcsán került a kutatás előterébe többek között a többugrásos *(multi-hop)* vezeték nélküli hálózat fogalma. Ezen hálózatok reprezentáns képviselője az úgynevezett ad hoc hálózat [5], melyben a résztvevők előre telepített hálózati infrastruktúra igénybevétele nélkül, önszervező módon hozzák létre és működtetik a hálózatot. Infrastruktúra hiányában az alapvető hálózati funkciókat maguk a résztvevők látják el. Ennek megfelelően, a kommunikáció többugrásos vezetéknélküli kommunikációra épül, ahol két távoli kommunikáló fél forgalmát más, földrajzilag a két kommunikáló fél között elhelyezkedő résztvevők továbbítják. Az adatforgalom továbbításán kívül a résztvevők egyéb hálózati szolgáltatást is nyújthatnak egymásnak. Alapvető tulajdonságainál fogva – ezen belül is a fix infrastruktúrától való függetlenségének köszönhetően – az ad hoc hálózati technológia várhatóan fontos szerephez jut majd a jövőben, mint a mindenütt jelenlevő számítástechnika vízióját támogató új generációs hálózati technológia.

Az ad hoc hálózati technológia számos biztonsággal kapcsolatos problémát vet fel [3].

Ezen problémák alapvetően két csoportba sorolhatók. Egyrészt az adatbiztonság és az adatvédelem hagyományos problémáit (hitelesítés, integritás védelem, titkosság, rendelkezésre állás, anonimitás stb.) kell egy teljesen új környezetben – azaz új feltevések mellett – megoldani. Másrészt számos eredendően új biztonsági probléma is felmerül, mely a hagyományos informatikai és távközlési rendszerekben egyszerűen nem létezik, vagy csak elhanyagolható mértékben van jelen.

A BME Híradástechnikai tanszékén, a CrySyS Laboratóriumban mindkét csoport problémáit vizsgáljuk kutatási programunk keretében (részletes leírást lásd a *www.crysys.hu* oldalon). Ezen cikk keretein belül azonban csak egy speciális problémával, nevezetesen a kooperációra való ösztönzés problémájával foglalkozunk.

Az ad hoc hálózat működése – és így az általa nyújtott szolgáltatások rendelkezésreállása is – arra a feltevésre épül, hogy a hálózat résztvevői kooperatívan viselkednek, azaz hajlandóak egymás számára szolgáltatásokat nyújtani. Ezt azonban semmi nem garantálja. Éppen ellenkezőleg: mivel a kooperatív viselkedés szolgáltatások nyújtását (pl. mások csomagjainak továbbítását) jelenti, ami viszont energiafogyasztással jár, a tipikusan telepről üzemelő résztvevők telepük élettartamának növelése érdekében esetleg megtagadhatják az együttműködés. Annál is inkább, mert a kooperatív viselkedés önmagában még nem garantálja egy adott résztvevő számára, hogy a többi résztvevő is kooperativan fog viselkedni vele szemben. Valójában, egy önző résztvevő parazita módon kihasználhatja a hálózat kooperáló résztvevőit saját csomagjainak továbbítására anélkül, hogy ő maga egyetlen csomagot is továbbítana (vagy egyéb szolgáltatást nyújtana) mások számára. Ezért fontos valamilyen kooperációra ösztönző mechanimus bevezetése a hálózatba. Hasonló jellegű probléma hagyományos hálózatokban lényegében nem létezik.

Jelen cikkben először osztályozzuk a nem-kooperatív viselkedés fajtáit, majd röviden áttekintjük a kooperatív viselkedésre ösztönző megoldások típusait és azok jellemzőit. Végül összefoglaljuk két általunk javasolt megoldás főbb elemeit, ötleteit.

2. A nem-kooperatív viselkedés osztályozása

A nem-kooperatív viselkedésnek több fajtája is létezik, melyeket a következő módon osztályozhatjuk [10]:

Indokolt nem-kooperatív viselkedés.

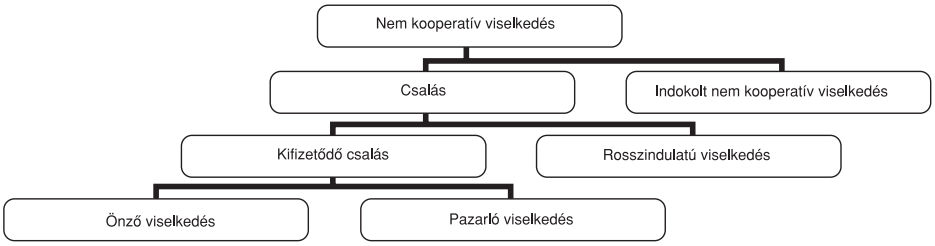
Az erőforrások szűkösségéből adódó nem-kooperatív viselkedés lehet átmeneti vagy állandó, attól függően, hogy az erőforrás hiánya átmeneti e vagy állandó. Állandó hiány akkor lép fel, ha az eszköznek nem áll rendelkezésére az erőforrás, például ha nincs elég számítási kapacitása vagy memóriája. Átmeneti hiány akkor léphet fel, ha például hirtelen nagy forgalom zúdul rá. Ezekben az esetekben az ösztönző mechanizmusnak nem szabad büntetnie az eszközt. Ehhez fel kell ismerni az indokolt nem-kooperatív viselkedést, és meg kell azt különböztetni az indokolatlan nem-kooperatív viselkedéstől.

Rosszindulatú viselkedés.

A rosszindulatú viselkedés egy nem kifizetődő viselkedési forma, ezért csak akkor fordulhat elő, ha egy magasabb rétegnek az előnyös. Például egy hírnév alapú hálózatban rágalmazó üzeneteket küldeni nem kifizetődő a hálózati réteg számára, viszont jó lehet az alkalmazási réteg számára, ha ezzel egy vetélytársát ki tudja zárni a hálózatból.

Önző és pazarló viselkedés.

Az önző és a pazarló viselkedés kifizetődő viselkedési forma. Egy forrás pazarlóan viselkedik, ha elárasztja a hálózatot fölösleges üzenetekkel, míg egy továbbító eszköz önző, ha nem továbbít csomagokat, pedig lenne rá módja.



Ebben a cikkben elsősorban az önző viselkedés megakadályozását célzó ösztönző sémákkal foglalkozunk.

3. Ösztönző sémák díjazási típusai

Az ösztönző sémák legfontosabb eleme a díjazás. A megbízó fizet a megbízottnak, hogy az számára valamilyen feladatot elvégezzen, például számításokat hajtson végre vagy csomagokat továbbítson. A díjazásnak két alapvető típusa terjedt el széles körben: a *hírnév alapú* és a *számla alapú* díjazás.

Hírnév alapú díjazás esetén a térítés mértéke függ az entitás hírnevétől. Az *A* entitás szempontjából a *B* entitás hírneve *A*-nak *B*-vel kapcsolatos tapasztalataiból és a többi entitás *B*-vel kapcsolatos tapasztalataiból ered. Az *A* entitás *B*-vel kapcsolatos bizalmát pedig *B* hírneve határozza meg dinamikus bizalmi séma alkalmazásával. Egy entitás hírneve csak a vele korábban kapcsolatba került entitások által ismert, illetve a hírnév szétárasztása által a környező entitások is ismerhetik. Ebből látható, hogy a jó hírnév csak stabil vagy lokalizált interakciós minták esetén kifizetődő. Hírnév alapú díjazási séma használata esetén a díjazásban való megegyezés fázisa kimarad, mivel a térítés mértékét a megbízó egyedül határozza meg. A hírnév valódi pénzzé konvertálása egyelőre nem megoldott, így ezen séma pénzügyi alkalmazása erősen korlátozott. Hírnév alapú ösztönzési sémákra számos példa található az irodalomban (pl. [2, 9]).

Számla alapú díjazás esetén minden entitás rendelkezik egy számlával egy virtuális banknál. A megbízó minden tranzakciónál kibocsát egy csekket, mellyel a megbízott a virtuális bank közreműködésével visszatérítést kap az elvégzett feladatokért. A bank elérhetősége előfeltétele a módszer helyes működésének, ezért szokás azt több kisebb lokális bank csomópontra partícionálni. Előfordulhat, hogy az entitás maga tárolja a saját számláját. Ehhez olyan modulokat kell az entitásokba beépíteni, melyek minden szempontból megbízhatóak. A számla alapú díjazás egy statikus bizalmi séma. Mivel minden entitás saját számlával rendelkezik, egyszerű a díjak valódi pénzzé átváltása. A probléma az lehet, hogy a számla alapú díjazás vagy megbízható hardverre, vagy a bank csomópontok elérhetőségére épít, s ez ad hoc hálózatokban külön nehézségeket jelent. Számla alapú ösztönző sémákra is számos példa található (pl. [1, 4, 6, 12]). Ezek közül kettőt részletesebben is bemutatunk a következő fejezetben.

4. Példák számla alapú ösztönzési sémákra

4.1. Csomagtovábbítás ösztönzése tiszta ad hoc hálózatokban

A [4]-ben egy olyan módszert javaslunk a kooperatív viselkedés ösztönzésére, mely számla alapú díjazásra épül és nem használ virtuális bankot (azaz az eszközök tárolják a saját számlájukat). Ehhez természetesen biztosítani kell valamilyen fizikai hozzáférésvédelmet, ami megakadályozza, hogy az eszköz gazdája hozzáférjen az eszközön tárolt számlához és manipulálni tudja azt.

Egy lehetséges megoldás az lenne, ha az egész eszköz manipulálás-ellenálló hardverre épülne, ám ez nehezen kivitelezhető és drága is. Az általunk javasolt megoldás csak annyit követel meg, hogy minden eszköz rendelkezzen egy manipulálás-ellenálló hardver modullal. Ez nem teljesíthetetlen követelemény, hiszen a mai mobil telefonokban is van ilyen modul, mégpedig a SIM kártya. A továbbiakban az eszközökben található manipulálás-ellenálló modult *biztonsági modulnak* nevezzük. A biztonsági modulról tehát azt feltételez-

zük, hogy az abban futó programok működését az eszköz gazdája nem tudja módosítani, azaz azok helyesen, az előírt protokollnak megfelelően működnek. Ugyanakkor megengedjük, hogy az eszköz gazdája az eszköz biztonsági modulon kívüli részének működését teteszőlegesen módosítsa. Az általunk javasolt megoldás azonban biztosítja, hogy az eszköz gazdájának semmi haszna nem származik az eszköz működésének módosításából, ezért feltehetően csak ritkán fog élni ezzel a lehetőséggel. Ezt a kritikus és nem kritikus funkciók körültekintő szétválasztásával és megfelelő kriptográfiai protokollok alkalmazásával érjük el.

A biztonsági modulra épülő ösztönző séma működését a következő módon foglalhatjuk össze röviden. Minden eszköznek van egy számlálója, melyet a biztonsági modul kezel, így ahhoz az eszköz gazdája nem fér hozzá. Ezt a számlálót *nuglet* számlálónak nevezzük. Mikor az eszköz egy saját csomagot szeretne küldeni, akkor azt először át kell adnia a biztonsági modulnak, ami egy kriptográfiailag védett fejlécet generál a csomag számára. Ezen kívül, a biztonsági modulban fut az útvonalválasztó algoritmus is, és így a modul meg tudja állapítani (vagy becsülni), hogy hány eszközön kell majd a csomagnak áthaladnia, amíg megérkezik a címzetthez. Jelöljük a szükséges továbbító eszközök (becsült) számát *n*-nel. Mielőtt a biztonsági modul kiadná a csomag elküldéséhez szükséges biztonsági fejlécet, ellenőrzi, hogy a nuglet számláló értéke nem kisebb-e, mint *n*. Ha igen, akkor a csomagot nem lehet elküldeni (nincs rá fedezet), és így a biztonsági modul nem adja ki a fejlécet az eszköz számára. Ha a nuglet számláló értéke nagyobb, mint *n*, akkor a biztonsági modul *n*-nel csökkenti azt, majd kiadja a fejlécet az eszköznek.

Ezek után az eszköz elküldi a csomagot a biztonsági fejléccel együtt. Minden továbbító eszköz a biztonsági fejléccel együtt átadja a csomagot a saját biztonsági moduljának. A modul csak akkor fogadja el a csomagot, ha a fejlécben található kriptográfiai ellenőrzőösszeg helyes. Ekkor a biztonsági modul új fejlécet generál a csomaghoz, melyet majd a következő továbbító eszköz biztonsági modulja fog ellenőrizni, és átadja az új fejlécet a továbbító eszköznek. Ezen kívül, a biztonsági modul feljegyzi, hogy a megelőző eszköznek (ha az nem maga a forrás volt) jár egy nuglet a csomag továbbításáért. Ezeket a feljegyzéseket minden szomszédra külön összegezve nyílvántartja a biztonsági modul, majd minden szomszéddal periodikusan futtat egy nuglet szinkronizációs protokollt, melynek segítségével a két szomszéd kiegyenlíti „tartozásait” egymás felé.

Vegyük észre, hogy egy továbbító eszköz csakis akkor kaphat fizetséget a csomag továbbításáért, ha valóban továbbította azt, hiszen mindig a következő eszköz biztonsági modulja jegyzi fel a továbbításért járó nuglet-et, ehhez azonban a csomagnak épségben meg kell érkeznie a következő eszközhöz. Azt is vegyük észre, hogy ha a csomag fejléce helytelen (vagy hiányzik), akkor a biztonsági modul nem fogadja el a csomagot, és így a továbbító eszköz nem kapja meg a továbbításért járó nuglet-et. Ezért egyetlen eszköznek sem áll érdekében fejléc nélküli vagy hibás fejlécű csomagot továbbítani. A csomag forrása tehát nem kerülheti el, hogy a csomagot elküldés előtt átadja a biztonsági moduljának (hiszen csak az tudja a megfelelő fejlécet generálni) és ezzel együtt fizessen a csomag elküldéséért.

A fent leírt ösztönző séma működését szimulációval elemeztük (a részleteket lásd [4]-ben). A szimulációban minden eszköz konstans átlagos sebességgel generál csomagokat véletlenül választott cél eszközök számára. Ha egy eszköz egy saját csomagot a nuglet számláló alacsony értéke miatt nem tud a generálás után azonnal elküldeni, akkor az eszköz eldobja a csomagot (azaz nem használ puffert a csomag ideiglenes tárolására). Minden eszköz célja az, hogy minimalizálja az eldobott saját csomagok számát. Több heurisztikus csomagtovábbítási stratégiát vizsgáltunk a fenti feltevések mellett, és a szimulációk eredménye azt mutatta, hogy a kooperatívabb stratégiák általában jobb teljesítményt értek el (a fenti cél tekintetében), mint a kevésbé kooperatívak. Más szavakkal, a javasolt eljárás valóban csomagtovábbításra ösztönzi az eszközöket, legalábbis a fenti feltevések mellett.

4.2. Csomagtovábbítás ösztönzése többugrásos celluláris hálózatokban

A többugrásos celluláris hálózat [7] abban különbözik a tiszta ad hoc hálózattól, hogy a celluláris hálózatokhoz hasonlóan bázisállomásokból, és az azokat összekötő nagy sebességű genrinchálózatból álló infrastruktúrára épül. Ugyanakkor, a mai cellás rendszerektől eltérően a mobil eszközök általában nem közvetlenül kommunikálnak a bázisállomással, hanem más mobil eszközök csomagtovábbító szolgáltatását igénybe véve, több „ugráson” keresztül érik el azt. Tipikus esetben a csomag útja a forrástól a cél eszközig a következő:

- a forrástól a forráshoz legközelebbi bázisállomásig mobil eszközök továbbítják a csomagot valamilyen, ad hoc hálózatokban is alkalmazott útvonalválasztó és csomagtovábbító technikát használva,
- a forráshoz legközelebbi bázisállomástól a célhoz legközelebbi bázisállomásig a gerinchálózaton halad a csomag,
- végül a célhoz legközelebbi bázisállomástól a célig ismét több mobil eszköz továbbítja a csomagot ismét ad hoc hálózati technológiát használva.

Látható tehát, hogy a tiszta ad hoc hálózatokhoz hasonlóan, a többugrásos celluláris hálózatok működése is feltételezi, hogy az eszközök kooperatívak, és továbbítják más eszközök csomagjait. Ezért a kooperációra való ösztönzés itt is fontos. Ebben az esetben azonban a megoldás formája annyiban módosul, hogy a résztvevők halmaza kibővül a bázisállomásokkal, pontosabban az azokat működtető hálózati szolgáltatóval, mely különböző biztonsági politikák betartatásával bizonyos mértékig kontrollálni tudja a hálózat működését. A kooperációra ösztönző eljárások természetesen

kihasználhatják a hálózati szolgáltató jelenlétét. A hálózati szolgáltató például könnyen játszhatja a virtuális bank szerepét, és ezzel olyan számla alapú díjazásra épülő ösztönző rendszer kialakítását teszi lehetővé, mely nem igényel manipulálás-ellenálló modult a mobil eszközökben.

A [6]-ban egy igen hatékony, probabilisztikus mikrofizetési sémára épülő ösztönző rendszert javasoltunk, mely többugrásos celluláris hálózatokban használható. Ez a csomagtovábbításra ösztönző eljárás azt feltételezi, hogy a mobil eszközök és a bázisállomás közötti kommunikáció aszimmetrikus abban az értelemben, hogy a mobil eszközök több ugráson keresztül érik el a bázisállomást, míg a bázisállomás közvetlenül tud forgalmazni a cellájában tartózkodó mobil eszközök felé. A javasolt eljárás a csomagtovábbítás ösztönzése mellett azt is lehetővé teszi, hogy a hálózati szolgáltató detektálja és azonosítsa a csalást megkisérlő mobil eszközöket.

A probabilisztikus mikrofiztés ötletét a következőképpen magyarázhatjuk el röviden [11]: Tegyük fel, hogy *A* szeretne *B*-nek fizetni egy kis összeget, mondjuk 1 Forintot. A hagyományos mikrofizetési sémákban *A* ezt úgy teszi meg, hogy átad *B*-nek egy 1 Forintot érő elektronikus zsetont, amit *B* valódi pénzre vált be a virtuális bank segítségével. Ezzel szemben, probabilisztikus mikrofizetés esetén *A* egy 1000 Forintot érő elektronikus lottószelvényt ad át *B*-nek, amely azonban csak 1/1000 valószínűséggel nyer. Az átadott szelvény várható monetáris értéke tehát pontosan 1 Forint.

A probabilisztikus séma előnye abból származik, hogy az átadott szelvény az esetek nagy többségében nem nyer, és így *B* nem fordul a virtuális bankhoz, hogy valódi pénzre váltsa az elektronikus szelvényt. Más szavakkal, a bank terheltsége nagy mértékben csökken. Ugyanakkor, ha *B* egy szolgáltató, aki sok felhasználóval bonyolít le a fentihez hasonló tranzakciót, akkor átlagosan ugyanannyit keres, mint a hagyományos fizetési sémát használva (feltéve, hogy az egyes lottószelvények nyerése egymástól független események). Ha *A* is sok tranzakciót bonyolít le (ami mikrofizetés esetén tipikus), akkor átlagosan ő sem veszít semmit egy hagyományos mikrofizetési séma használatához képest. Az *A*-ra eső fluktuációt (néha többet kell fizetnie, mint amennyit valójában vásárolt) ki lehet küszöbölni [8].

A [6]-ban javasolt ösztönző séma alapötlete, hogy a csomag forrása egy elektronikus lottószelvényt csatol a csomaghoz, mely egy meghatározott *p* valószínűséggel nyerő szelvény bármely továbbító eszköz számára, ahol *p* egy rendszer-paraméter, amit a hálózati szolgáltató állít be. Minden, a csomagot továbbító eszköz ellenőrzi, hogy számára a csatolt szelvény nyerő-e vagy sem. A nyerő szelvényeket a továbbító eszköz tárolja. A nyerő szelvénnyel együtt azt is megjegyzi, hogy a szelvényt tartalmazó csomagot melyik eszköztől kapta és melyik eszköznek küldte tovább.

Az összegyűjtött nyerő szelvényeket, valamint a velük együtt tárolt eszköz-azonosítókat, az eszköz egy későbbi időpontban, kötegben átadja a hálózati szolgáltatónak (például mikor az eszköz fizikailag közel kerül egy bázisállomáshoz és így közvetlenül el tudja a köteget küldeni a bázisállomásnak). A bázisállomás a köteget a hálózati szolgáltató számlázó központjába küldi.

Mikor egy csomag megérkezik a bázisállomáshoz, a bázisállomás ellenőrzi a csomaghoz csatolt lottószelvény érvényességét (a lottószelvény nem más, mint egy üzenethitelesítő kód, melyet a forrás és a hálózati szolgáltató közötti titkos kulcs segítségével számol ki a forrás és ellenőriz a bázisállomás; a továbbító eszközök számára ez a kód egy pénzfeldobás sorozat). Ha a szelvény érvényes (azaz valóban a csomag forrása generálta), akkor a csomagot a bázis állomás továbbítja a cél felé. Ellenkező esetben a bázisállomás eldobja a csomagot, hiszen annak továbbításáért nem tud megterhelni senkit.

A sikeres csomagokról a bázisállomás tájékoztatja a hálózati szolgáltató számlázási központját. A számlázási központ tehát két forrásból kap információt: egyrészt a bázisállomások tájékoztatják, hogy mely csomagok érték el sikeresen a célt, másrészt a továbbító eszközök küldik el nyerő lottószelvényeiket. A számlázási központ ezen információk összevetésével állapítja meg, hogy kit kell megterhelni, kit kell kifizetni, és hogy ki próbált meg csalni. Egészen pontosan, a sikeres csomagok forrásának számláját a központ megterheli. A terhelés mértékét a hálózati szolgáltató állapítja meg, ám az alapvetően a csomag méretétől függ.

A nyerő szelvényekre csak akkor fizet a központ, ha a szelvényhez tartozó csomagot valamely bázisállomás jelentette, azaz az sikeresen elérte a célt. Ez ösztönzi az eszközöket, hogy továbbítsák a csomagot, különben nem kapnak fizettséget, hiába rendelkeznek nyerő szelvénnyel. Ráadásul mikor egy nyereményt kifizet a központ, akkor nemcsak a nyerő szelvényt benyújtó eszköznek fizet, hanem annak eszköznek is, amelytől a szelvényt benyújtó eszköz a csomagot kapta, és annak is, akinek a csomagot továbbküldte. Ez még jobban ösztönzi az eszközöket a csomagok továbbítására, hiszen így még vesztes szelvényt tartalmazó csomagokat is van értelme továbbítani, mivel ugyanaz a szelvény a következő eszköz számára lehet nyerő, mely esetben a nem nyerő továbbító eszköz is jutalomban részesül.

A fentieken túl, a szomszédok nyerő szelvénnyel együtt történő lejelentésének van egy másik előnye: lehetővé teszi a központ számára csomagtovábbítási statisztikák készítését. Az ezen statisztikákban felfedezett inkonzisztencia pedig lehetővé teszi a csalások detektálását, majd megbüntetését. Ha például egy eszköz szisztematikusan megtagadja a csomagok továbbítását, akkor nagyobb gyakorisággal fog megjelenni csomagot fogadó szomszédként, mint csomagot küldő szomszédként. Ráadásul, minnél agresszívebben tagadja meg egy eszköz a csomagok továbbítását, annál könnyebben és hamarabb fogja ezt a számlázási központ detektálni.

Irodalom

[1] N. B. Salem, L. Buttyán, J.-P. Hubaux, M. Jakobsson: A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks, In Proceedings of the 4th ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Annapolis, Maryland, USA, 2003.

[2] S. Buchegger, J.-Y. Le Boudec: Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc NeTworks), In Proceedings of the Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, June 2002.

[3] L. Buttyán, J.-P. Hubaux (eds.): Report on a Working Session on Security in Wireless Ad Hoc Networks, ACM Mobile Communications and Computing Reviews, 7(1), 2003.

[4] L. Buttyán, J. P. Hubaux: Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks, ACM/Kluwer Journal on Mobile Networks and Applications (MONET), to appear, October 2003.

[5] S. Corson, J. Freebersyser, A. Sastry (eds.): ACM/Kluwer Mobile Networks and Applications, Special Issue on Mobile Ad Hoc Networking, October 1999.

[6] M. Jakobsson, J.-P. Hubaux, L. Buttyán: A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks, In Proceedings of the Seventh International Financial Cryptography Conference, Guadeloupe, January 2003.

[7] Y.-D. Lin, Y.-C. Hsu: Multihop Cellular: A New Architecture for Wireless Communications, In Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom), Tel Aviv, 2000.

[8] S. Micali, R. Rivest: Micropayments Revisited. In Proceedings of the Cryptographer's Track at the RSA Conference, 2002.

[9] P. Michiardi, R. Molva: CORE: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks, In Proceedings of the IFIP Communication and Multimedia Security Conference, Portoroz, Slovenia, 2002.

[10] P. Obreiter, B. Koenig-Ries, and M. Klein: Stimulating cooperative behavior of autonomous devices – an analysis of requirements and existing approaches, In Proceedings of the Second International Workshop on Wireless Information Systems (WIS), 2003.

[11] R. Rivest: Electronic Lottery Tickets as Micropayments, In Proceedings of the Financial Cryptography Conference, 1997.

[12] S. Zhong, Y. R. Yang, and J. Chen: Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad Hoc Networks. In Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom), 2003.

Hírek

Az **Invitel Rt.** és az **Ericsson Magyarország** keretszerződést írt alá **Ethernet DSL Access** (EDA) rendszer telepítésére és rendszerintegrációs munkákra. A közelmúltban az Ericsson mérnökei olyan megoldást fejlesztettek ki, amellyel a szolgáltatók minden eddiginél olcsóbban, gyorsabban és egyszerűbben építhetik ki saját ADSL hálózartukat.
Az EDA technológia lényege, hogy nincsen szükség viszonylag drága ATM alapú felhordóhálózatra, mert helyette a már jól megszokott Ethernet hálózati elemek használhatók. Az Ethernet DSL Access technológia egészen kicsi, 10-12 előfizető kiszolgálására alkalmas dobozokból épül fel.

2003. február végétől **Axelero Internet Biztonság** néven új szolgáltatást indított az **Axelero** az **F-Secure Corporation**-nel együttműködve, amely védelmet nyújt a személyi számítógépeket érő különféle külső támadásokkal és vírusokkal szemben. Az egyedi konstrukcióban kínált szolgáltatást az Axelero minden jelenlegi és új hozzáférést vásárló előfizetője egyaránt igénybe veheti, havi nettó 1000 forintos előfizetési díj ellenében.
Az Axelero új akciója révén a február 16. és március 31. között ADSL Profi hozzáférést vásárlók ingyenesen juthattak a szolgáltatáshoz. A vállalat előjelzése szerint ez év végéig közel 7000 előfizető veszi igénybe majd az új biztonsági megoldást.