Adatbiztonság elemzése mobil WiFi környezetben

Orosz Péter, oroszp@delfin.unideb.hu
Gál Zoltán, zgal@cis.unideb.hu
Karsai Andrea, kandrea@fox.unideb.hu

Debreceni Egyetem Informatikai Központ

1. Bevezetés

A helyi hálózatokra tervezett adatkommunikációs technológiák világában a vezeték nélküli átviteli mechanizmusok térnyerésüket a nagyfokú mobilitásnak köszönhetik. A rádiós adatátvitel ugyanakkor komplex adatbiztonsági kérdéseket vet fel a szakemberek számára. Kérdés, hogy a jelenleg elérhető biztonsági technológiák (WPA, WPA2), illetve EAP alapú hitelesítési (PEAPv0, v1) és adatforgalom-titkosító (TKIP, AES-CCMP) protokollok alkalmazása milyen mérhető hatással van a mobil WiFi rendszer átviteli jellemzőire, különös tekintettel a mozgásban lévő mobil terminál cellaváltáskor bekövetkező L2 roaming folyamatának időtartamára.

Korábbi vizsgálatok alapján tudjuk, hogy a mobil kliens fizikai mozgása közben bekövetkezett cellaváltás – különböző mértékben, de – hatással van mind a TCP mind az UDP forgalomra[1]. Ekkor zajlik le adatkapcsolati szinten a roaming folyamat, mely során a mobil terminál az előző cella bázisállomásáról lekapcsolódva, az aktuális fizikai helyén elérhető, legelőnyösebb vételi paraméterekkel rendelkező bázisállomáshoz kapcsolódik. Ezek után kulcsfontosságú a már hitelesített kliens újrahitelesítése, melyre a fejlettebb EAP mechanizmusok lehetőséget adnak. Kérdés, hogy az újrahitelesítés, kulcs generálás mennyivel növeli meg a roaming hatására bekövetkezett forgalomkiesés időtartamát, illetve milyen viselkedést mutatnak a felsőbb rétegek protokolljai a rádiós átviteli közegben végbemenő adatvesztés következtében?

Az adatforgalom titkosítására alkalmazott, a kor biztonsági követelményeinek megfelelő titkosító protokollok (TKIP, AES-CCMP) dinamikusan cserélik a mobil kliensekhez rendelt kulcsokat. Az előadásban megvizsgáljuk, hogyan viselkednek az említett protokollok a cellaváltás időtartama alatt. A gyakorlatban felállított WiFi tesztkörnyezetben végzett vizsgálatok ezekre a kérdésekre próbálnak választ adni.

2. WiFi biztonsági technológiák áttekintése

WPA

Az IEEE 802.11b szabvány eredeti biztonsági mechanizmusa (WEP) bizonyítottan nem tekinthető biztonságos titkosító megoldásnak[4]. Az IEEE hálózatbiztonsággal foglalkozó osztálya egy magas szintű biztonsági szabvány kidolgozását tűzte ki célul. Így született meg a 802.11i szabvány, melynek célja a 802.11 hálózatok biztonságossá tétele.

A WiFi Alliance egy korai verzióját alkalmazta az említett szabványnak (draft 3.0), kiemelve abból a biztonsági fejlesztések egy olyan részhalmazát, mely képes együttműködni a már létező hardvereszközökkel. Ezt nevezzük WiFi Protected Access (WPA) technológiának[3]. A 802.11 szabvány WEP algoritmust definiál a vezeték nélküli hálózatok védelmére. Az eredeti WEP 40 bites RC4 kulcsokat alkalmaz 24 bit inicializációs vektorral (IV), továbbá CRC32 algoritmussal védekezik a csomagbarkácsolás ellen. Azonban ezen algoritmusok mindegyikéről bebizonyosodott, hogy nem elegendőek a megfelelő biztonság eléréséhez. Például az IV hossza túl kicsi, így viszonylag rövid időn belül jó eséllyel újra megjelenthet egy adott érték. Ez a biztonsági hiba nagymértékben megkönnyíti a valósidejű visszafejtést. Továbbá újrajátszás/replay elleni védelmet sem építettek be.

A WPA valójában köztes megoldást ad a vezeték nélküli hálózatokban felmerülő biztonsági kérdésekre. A kulcsok menedzsmentje kétféle mechanizmus alapján történhet: 1. hasonlóan a 802.1x-hez a WPA is támogatja külső autentikációs szerver (pl. RADIUS) és EAP használatát[5]. 2. előre kiosztott (pre-shared) kulcsokkal oldja meg a hitelesítést. Az előbbit WPA-Enterprise-nak, míg az utóbbit WPA-PSK-nak vagy Personal-nak nevezzük. Mindkét mechanizmus master kulcsot generál a kliens (supplicant) és a bázisállomás (authenticator) számára. A WEP kiváltására TKIP (Temporary Key Integrity Protocol) protokollt definiál, mely kompromisszumnak tekinthető a biztonságos kommunikáció és a hardver-kompatibilitás között. A TKIP RC4 kriptográfiai algoritmust használ a titkosításhoz. Minden csomaghoz saját 128 bites (per-packet) RC4 kulcsot generál. Ezzel megakadályozza a kulcs megszerzésére irányuló (key recovery) támadásokat. Beépítettek a WPA-ba újrajátszás (replay) elleni védelmet is: Michael Message Integrity Code algoritmust.

A WPA új, négylépéses Key Handshake algoritmust vezet be a bázisállomás és a kliens közötti adatforgalom-titkosító kulcsok generálásához és cseréjéhez. Ez a mechanizmus arra is jó, hogy ellenőrizze valóban rendelkezik-e a master kulccsal a bázisállomás és a kliens. A TKIP protokoll további, részletes ismertetése a 3. fejezetben olvasható.

WPA2 / IEEE 802.11i

Időközben befejeződött az IEEE 802.11i hiányzó részeinek fejlesztése, így 2004 júniusában szabványosították. Ennek hatására a WiFi Alliance a végleges 802.11i-t alapul véve megalkotott egy továbbfejlesztett WPA verziót, melyet WPA2-nek nevezett el. Továbblépés a WPA-hoz képest a komplexebb, robosztusabb AES-CCMP (AES in Counter Mode with CBC-MAC Protocol) titkosító mechanizmus támogatása, mely egy speciális változata a standard AES-128 protokollnak.

3. Adattitkosító algoritmusok

TKIP

A TKIP protokollt a 802.11i szabvány definiálja. Tervezőinek köztes megoldást kellett találniuk a megfelelő szintű adatbiztonságot és a meglévő vezeték nélküli eszközökkel való együttműködést együttesen figyelembe véve. Ebből adódóan a protokoll ugyanazt az RC4 kódolási algoritmust használja, melyet a WEP-hez is meghatároztak, bár a TKIP által alkalmazott RC4 kódolás már 128 bites kulcsokkal dolgozik. Legfontosabb változás a WEP-hez képest, hogy minden egyes adatcsomaghoz saját kulcs generálódik (per-packet kulcs). A kulcsot különböző adatok keverésével hozzák létre: a küldő csomópont fizikai címétből és a csomag azonosítójából. Minden egyes csomag melyre alkalmazzuk a TKIP-t, rendelkezik egy 48 bites széria számmal, mely eggyel növekszik, amint egy újabb csomag kerül átvitelre. Az algoritmus ezt az értéket használja Inicializációs Vektorként (IV) és a kulcs részeként is. Ez a szekvencia szám biztosítja, hogy minden egyes csomaghoz külön kulcs tartozzon. Emellett, nem kevésbé jelentős továbblépés, hogy az alap kulcsot (base key) belekeveri a TKIP kulcsba.

A TKIP minden egyes kliens-bázisállomás unicast kommunikációhoz négy kulcsból álló kulcshalmazt rendel, valamint további két kulcsot a multicast, illetve broadcast forgalom számára[2].

Az eljárás a következő ideiglenes kulcsokat (PTK - Pairwise Transient Key) használja az unicast adatok titkosítására:

1. Data encryption kulcs: 128 bites kulcs az unicast keretek titkosítására.
2. Data integrity kulcs: 128 bites kulcs, mellyel kiszámolható a MIC az unicast keretekhez.
3. EAPOL-Key encryption kulcs: 128 bites kulcs az EAPOL-Key üzenetek titkosítására.

4. EAPOL-Key integrity kulcs: 128 bites kulcs, mellyel kiszámolható a MIC EAPOL-Key üzenetekhez.

A pairwise ideiglenes kulcsok (PTK) meghatározásához az alábbi értékeket használja a WPA:

1. Pairwise Master Key (PMK): 256 bites kulcs, melyet az EAP-TLS or PEAP hitelesítési eljárásból származtat.
2. Nonce 1: A bázisállomás által meghatározott véletlenszerű érték.
3. MAC 1: A bázisállomás MAC címe.
4. Nonce 2: A kliens által meghatározott véletlenszerű érték.
5. MAC 2: A vezetéknélküli kliens MAC címe.

A PMK-t az EAP hitelesítés során a hitelesítő (RADIUS) szerver és a vezeték nélküli kliens együttesen határozzák meg, majd a szerver eljuttatja a bázisállomáshoz egy Access-Accept üzenetben. Ezután az AP kezdeményezi a négylépéses Key Handshake algoritmust:

1. A bázisállomás küld egy Nonce1-et és a MAC1-et tartalmazó EAPOL-Key üzenetet. Mivel az ideiglenes unicast kulcsokat még nem határozták meg, ez az üzenet kódolatlan szöveges formában, integritási védelem nélkül jut el a klienshez. Ezáltal a kliens rendelkezni fog minden infromációval a pairwise ideiglenes kulcsok kiszámításához.
2. A mobil kliens visszaküld egy EAPOL-Key üzenetet, mely tartalmazza az Nonce2-t és a MAC2-t, továbbá a MIC értéket. A kliens kiszámította az ideiglenes kulcsokat, emellett meghatározza a MIC értéket is, felhasználva EAPOL-Key integrity kulcsot. A bázisállomás Nonce 2 and MAC 2 értékek alapján határozza meg az ideiglenes kulcsokat, és érvényesíti a MIC értékét.
3. Az AP ismételten küld egy EAPOL-Key üzenetet egy MIC értékkel és egy kezdeti szekvencia számmal. Ezzel jelzi, hogy készen áll titkosított unicast és EAPOL-Key üzenetek küldésére.
4. A mobil kliens visszaküld egy EAPOL-Key üzenetet egy MIC értékkel és egy kezdeti szekvencia számmal. Ezzel jelzi, hogy ő is felkészült titkosított unicast és EAPOL-Key üzenetek küldésére.

A fenti lépések kettős célt szolgálnak: 1. az ideiglenes kulcsok (PTK) meghatározása. 2. a kapott MIC értékkel ellenőrzhető, hogy mind a kliens, mind a bázisállomás ténylegesen rendelkezik-e a PMK-val.

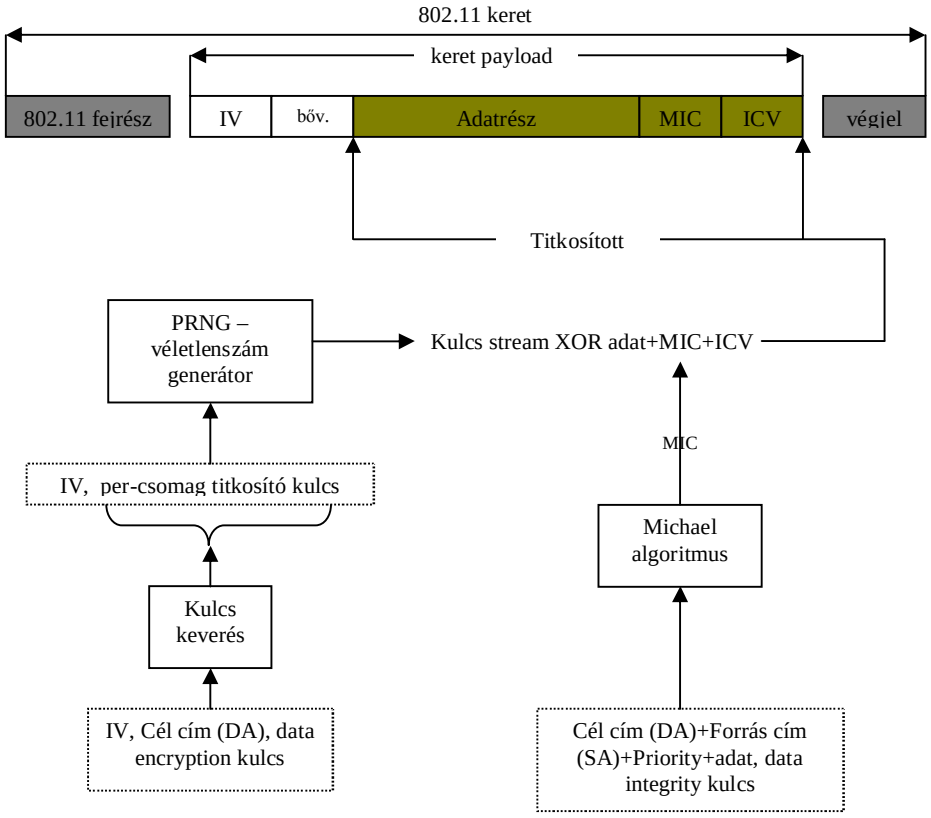
Az adatkeretek tikosításához az alábbi adatokra van szüksége a protokollnak:

- Inicializációs Vektor (IV).
- A PTK kulcsok közül a data encryption kulcs, vagy a group encryption kulcs.
- A keret cél- és forráscíme (DA, SA).
- A priority mező értéke, ami alapesetben “0”.
- A PTK kulcsok közül a data integrity kulcs, vagy a group integrity kulcs.

A TKIP titkosítási algoritmusa:

1. A WPA keverési funkciójának – amely kiszámítja a per-csomag kulcsot – bemenetei az IV, a DA, és a data encryption kulcsok lesznek.
2. A Michael adatintegritási algoritmus a MIC előállításához bemenetként a célcímet, a forráscímet, a priority értéket, az adatrészt (a titkosítás nélküli 802.11 payload), és a data integrity kulcsot alkalmazza.
3. Az ICV-t a CRC-32 checksum-ból határozza meg.

4. Az RC4 programozott véletlenszám generátorának (PRNG) bemenete az IV és a per-packet kulcs lesz. Ezekből állítja elő a generátor a kulcs stream-et, melyek mérete megegyezik az adatrész, a MIC és az ICV értékek együttes méretével.
5. A kulcs stream és az adatrész, MIC és ICV kombinációval elvégez egy logikai XOR műveletet, így hozza létre a titkosított 802.11 adatrészt.
6. Végül hozzáadja az IV-t az így kapott titkosított adatrészhez, majd az eredményt becsomagolja egy 802.11 fejrésszel és végjellel.



1. ábra A TKIP titkosítás blokksémája

AES-CCMP

A CCMP hasonlóan a TKIP-hez ideiglenes kulcsokat (PTK) alkalmaz az adatok titkosítására. A PTK meghatározásahoz a TKIP-nél már ismertetett 4 lépéses Key Handshake eljárást használja. Mivel tartalmaz adatintegritási védelmet, ezért egyszerre válthatja ki a TKIP-t és a Michael algoritmust. Az AES-CCMP a 802.11 payload és MIC titkosításához counter módú AES-t alkamaz, és a MIC meghatározását CBC-MAC algoritmussal végzi, az alábbiak szerint:

1. AES-sel titkosít egy 128bites kezdő blokkot és a data integrity kulcsot. Ez 128 bit hosszúságú kódot eredményez (X1).
2. Végrehajt egy XOR műveletet az előbbi 128 bites kódón és a következő 128 bites adatblokkon, miközben a MIC értéket is meghatározza. Az éredmény szintén egy 128 bites kód (X2).
3. Az X2 kódot titkosítja AES-sel a data integrity kulcsot felhasználva. Így létrejön X3.
4. Ismét XOR műveletet hajt verge X3-n és a következő 128 bites adatblokkon.

Az eljárás a 3. és 4. lépést ismétli minden újabb 128 bites adatblokkra. A 128 bites kód felső 64 bitje lesz a MIC érték.

4. A mérési környezet és a mért adatok ismertetése

A mérésekhez alkalmazott eszközök mindegyike képes IEEE 802.11a/b/g szabványoknak megfelelő kommunikációra, valamint támogatja az általunk tesztelt biztonsági technológiákat. Vizsgálatunk fókuszában a különböző biztonsági mechanizmusok és rádiós átviteli technológiák mozgó kliensre kifejtett együttes hatása állt. A mozgó kliens cellaváltásakor bekövetkező roaming folyamatot befolyásoló hatásokat mértük és elemeztük, ugyanis a roaming idő alatt kieső forgalom mértéke jelentősen befolyásolja a hálózati alkalmazások szolgáltatási minőségét. A mobil kliens 5-6 km/h (1,4-1,7 m/sec) sebességgel haladt a bázisállomásokat összekötő egyenessel párhuzamos irányban oda-vissza. Egy mérési periódus (TSi) alatt az MT L2 roaming hatására az AP1-ről az AP2-re asszociált, majd visszafelé haladva újabb L2 roaming hatására visszakerült az AP1 hatáskörébe. A mobil terminál egy notebook volt, amelyen FTP kliens futott. A TCP kapcsolat huzalos végén egy Linux alapú csomópontot helyeztünk el, melyen FTP szerver futott. Nagyméretű állományt mozgattunk a kliens és a szerver között. Az átviteli sebességet 256Kbyte/sec-re korlátoztuk, ami jól közelíti egy átlagosan (10-15 klienssel) terhelt bázisállomáson mérhető effektív felhasználói sávszélességet. Fájl letöltésre és feltöltésre is elvégeztük a méréseket, ugyanis a bázisállomás más-más viselkedést mutat a forgalom irányának megfelelően.

Mindkét bázisállomás ugyanabban az L2-es VLAN-ban helyezkedett el, fizikailag egymástól 50 méteres távolságban. Vezetékes oldalon a bázisállomások forgalmát tükröztük egy monitor VLAN-ba, ahol a kereteket egy Linux-os munkaállomáson tcpdump segédprogrammal kaptuk el, és mentettük le. A mért adatok elemzéséhez az Ethereal 10.0.14-es verzióját használtuk. A bázisállomások által kisugárzott rádiós teljesítményt 802.11b/g esetén 5mW-ra, míg 802.11a esetén 12mW-ra állítottuk be, figyelembe véve a méréshez szükséges optimális cellaméretet. Az említett IEEE 802.11a/b/g rádiós szabványokra először nyitott (open), hitelesítés nélküli kommunikációval végeztük el a méréseket, majd hitelesítéssel (PEAPv0, v1) és titkosítással (TKIP, CCMP) az alábbi táblázatban megadott protokoll-kombinációkat alkalmazva:

1. táblázat. Biztonsági technológiák

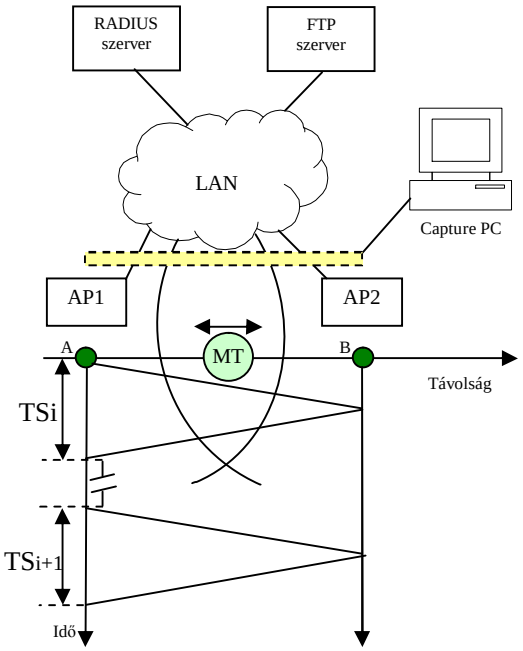
Technológia	*Autentikáció*	*Titkosítás*
WPA	PEAP-MSCHAPv2	TKIP
	PEAP-GTC	TKIP
WPA2	PEAP-MSCHAPv2	AES-CCMP
	PEAP-GTC	AES-CCMP

Az MT az A pontból haladt a B pontba, majd vissza. Az A és B pont közötti távolság 50 méter. A biztonsági technológiák roaming időtartamra, valamint TCP adatátvitelre gyakorolt hatásának vizsgálatához az alábbi időpillanatokat határoztuk meg. A cellaváltás időtartamát jelentősen befolyásolja a bázisállomások beacon periódusa. Korábbi vizsgálatainkból kiderült, hogy IEEE 802.11g/b esetén 50ms alatti periódusidővel érhető el a legkedvezőbb cellaváltási idő. Ennek megfelelően méréseinket b/g esetben 40ms-os beacon periódussal vegéztük. IEEE 802.11a esetén 50ms körüli értékkel kapunk elfogadható roaming teljesítményt. Ezért itt 50ms-ra állítottuk be a periódust.

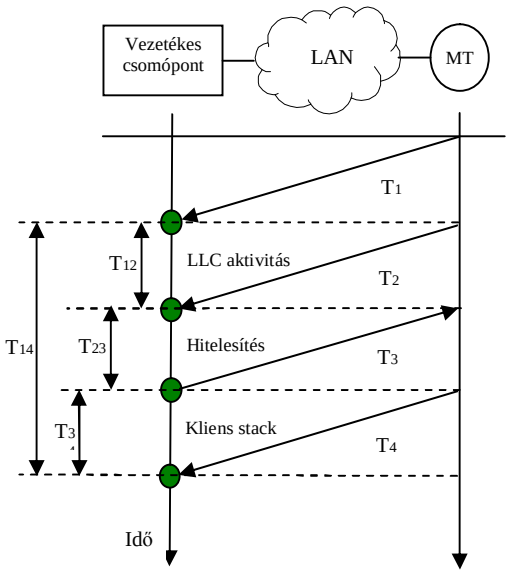
2. táblázat. Jelölésmagyarázat

Időpillantok	*Esemény leírása*
T_1	L2 roaming előtt az MT által küldött utolsó TCP csomag
T_2	Újrahitelesítés kezdete
T_3	Újrahitelesítés vége
T_4	L2 roaming után az MT által küldött első TCP csomag

Az első, T_{12} időtartam a L2-es roaming folyamat időtartama, ennek részleteit korábbi cikkünkben mutattuk be[1]. A T_{23} újrahitelesítési időtartam alatt végbemegy a 802.1x autentikáció a kliens és a RADIUS szerver között, meghatározzák a PMK-t, majd a bázisállomás és a kliens végrehajtja a 4 lépéses Key Handshake algortimust, mely az ideiglenes kulcsokat állítja elő az adatforgalom titkosításához.



2. ábra. Mérési környezet



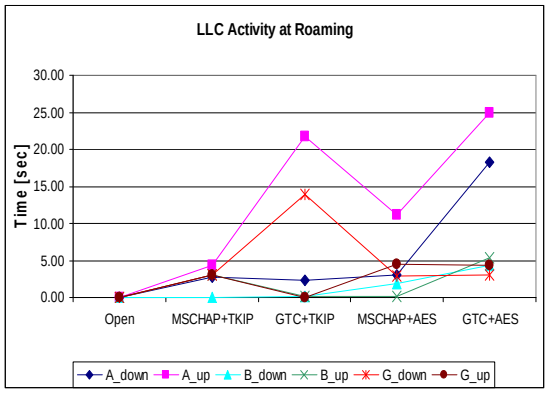
3. ábra. Mért időtartamok

Ezek után indulhat el a titkosított adatforgalom a kliens és a bázisállomás között. A cellaváltás alatt a legtöbb esetben nem szakadt le a TCP kapcsolat, viszont jelentős forgalomkiesést jelentkezhet. A T_{34} érték jól mutatja, hogy a TCP kapcsolat nem azonnal éled fel, az újrahitelesítés és az első hasznos TCP csomag között jelentős időkülönbségek adódhatnak (ez legfőképp a kliens TCP/IP stack-jének függvénye).

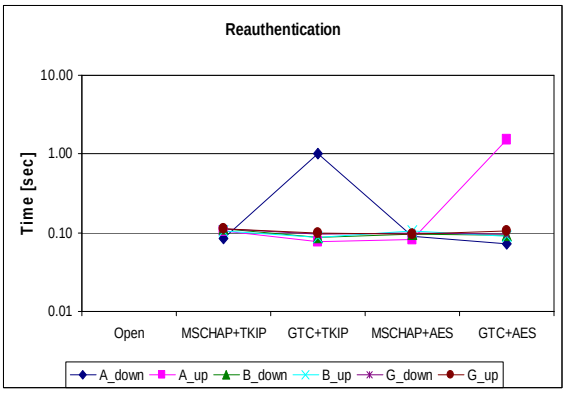
5. Az eredmények értelmezése

A méréskor a vezetékes oldal teljes adatforgalmát lementettük állományokba, így elemzéskor a roaming folyamatot jellemző jelenségekről teljesebb képet kaptunk. Az L2-es roaming folyamat alatt a mobil kliens jól meghatározható keretsorozatot küld az új bázisállomás irányába, így minden állományban egyszerűen meg tudtuk állapítani a roaming esemény időpontját. Mivel TCP forgalmat vizsgáltunk, így természetesen a legfontosabb kérdés az volt, hogy milyen hatásai lesznek a cellaváltás során végbemenő folyamatoknak a TCP adatfolyamra. Továbbá az is lényeges, hogy az eltérő rádiós technológiák milyen időtartambeli különbségeket mutatnak. Az alábbi grafikonokon a roaming folyamatot lépésire bontva mutatjuk be, hangsúlyozva a forgalom irányának fontosságát. Bármely részfolyamatot vizsgáljuk, szignifikáns különbségek figyelhetők meg az egyes hitelesítési mechanizmus (MSCHAP és GTC) és rádiós technológia (IEEE 802.11a/b/g) kombinációk között. Az LLC aktivitás időtartama nagymértékben függ az alkalmazott PEAP típustól (4. ábra). Itt az MSCHAP minden esetben gyorsabb L2 roamingot

eredményezett. Érdemes megfigyelni azt is, hogy az időtartam a TCP forgalom irányának is függvénye.



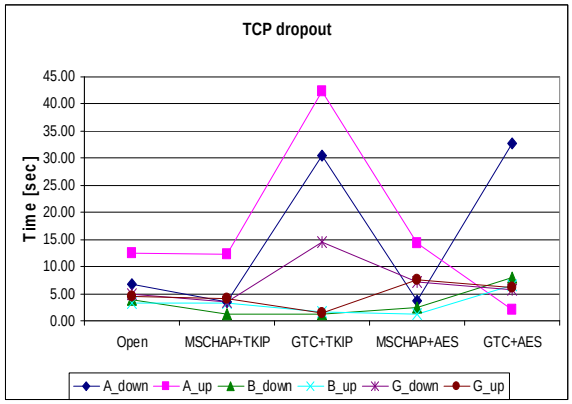
4. ábra. L2 roaming időtartam



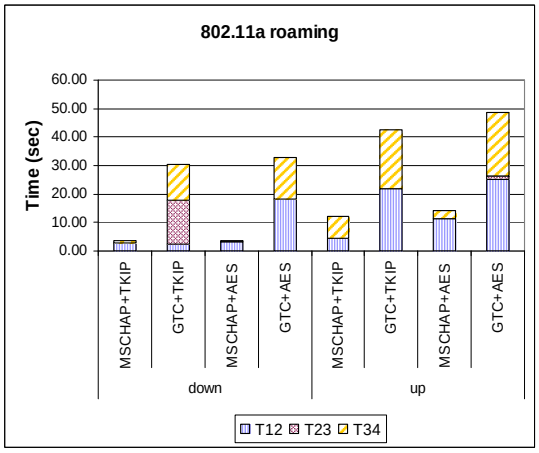
5. ábra. Az újrahitelesítés időtartama

Az újrahitelesítési szakaszban jóval kisebb (<20ms) az eltérés a hitelesítési mechanizmusok között (5. ábra). Minden hitelesítési időtartam 100ms körül ingadozik. A két autentikációs protokoll közti különbség magyarázata az, hogy az MSCHAP titkosított formában cseréli az üzeneteket, a GTC viszont titkosítás nélkül. Az MSCHAP hitelesítéskor megjelenő számítási többlet ennek ellenére nem jelentős. A grafikonon látható extrém eltérések sokkal inkább a rádiós technológiák közötti különbségekre világítanak rá. Az IEEE 802.11a szabvány minden mérési intervallumban gyengébben teljesített a 802.11b/g technológiákhoz képest. Szélsőséges esetekben (802.11a+GTC+TKIP, 802.11a+GTC+AES) az újrahitelesítés időtartama (~1000ms) egy nagyságrenddel nagyobb az átlagosan mért 100ms-os értéknél. A TCP forgalomkiesés irányérzékeny, mivel a bázisállomás pufferelést végez a beérkező csomagokra. Két eltérő karakterisztikájú hálózattípust kapcsol össze, ezért az alkalmazott pufferméret és a pufferkezelési algoritmus egyértelműen meghatároza az állomás roaming teljesítményét.

A teljes TCP forgalomkiesést a 6. ábra szemlélteti. A grafikon a kliens által a régi bázisállomásnak küldött utolsó és az új bázisállomás irányába küldött első hasznos TCP csomag közötti intervallumokat mutatja. A legkedvezőtlenebb értékek a 802.11a és GTC hitelesítés kombinációjával adódtak. Viszont az is látszik, hogy elfogadható eredmény érhető el 802.11g/b és PEAP-MSCHAP/GTC együttes alkalmazásával, egyes esetekben (MSCHAP/GTC+TKIP, MSCHAP+AES) az open autentikációt megközelítő értékek adódtak a roaming folyamat időtartamára.

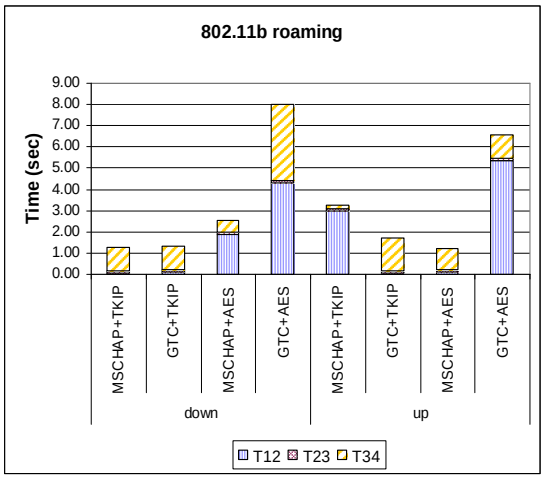


6. ábra. A teljes TCP forgalomkiesés

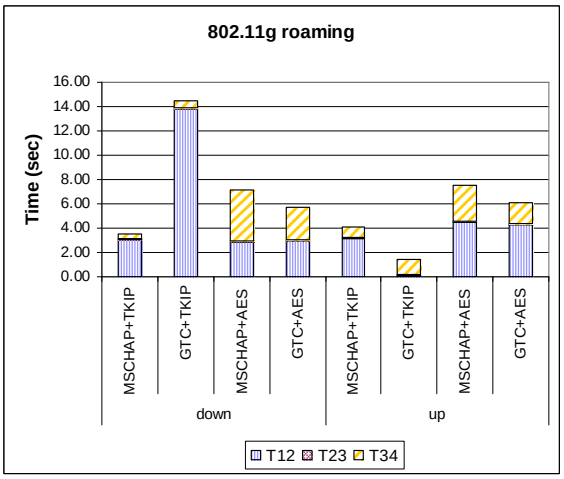


7. ábra. Hitelesítés és titkosítás 802.11a esetén

Ha összevetjük az IEEE 802.11 rádiós technológiák roaming teljesítményét (7.,8.,9. ábra), azt tapasztaljuk, hogy a legkedvezőtlenebb értékek 802.11a szabvány esetén jelentkeznek. Ennek egyik oka, hogy a mikrocellák mérete ennél a technológiánál kisebb, mint az azonos sugárzási teljesítményű 802.11b/g állomások esetén. Az 50 méteres távolságban levő bázisállomások cellái kevésbé vannak átfedésben. (Ennek ellensúlyozására növelhetjük a kisugárzott rádiós teljesítmény, ekkor viszont ügyelni kell arra, hogy az 5,4GHz-es tartományban üzemelő 802.11a szabvány jóval alacsonyabb maximális adóteljesítményt tesz lehetővé: 40mW.)



8. ábra. Hitelesítés és titkosítás 802.11b esetén



9. ábra. Hitelesítés és titkosítás 802.11g esetén

6. Összefoglalás

Az IEEE 802.11 rádiós szabványok cellaváltás közbeni viselkedésének vizsgálata irányadó lehet olyan védett vezeték nélküli LAN hálózatok tervezésénél, melyekben a mobilitási funkció kiemelt fontosságú. Látható, hogy az IEEE 802.11a szabvány nem bizonyult hatékony technológiának a mobilitás tekintetében. Amellett, hogy jelentősen nagyobb időtartamok adódtak a roaming részfolyamatokra, a cellaváltás számos esetben a TCP kapcsolat szakadását idézte elő. A hitelesítési és titkosítási mechanizmusoknál tapasztalható eltérések mértéke jóval kisebb nagyságrendű. Az eltérés az algoritmusok közti komplexitási különbségekkel, az eltérő számítási igényekkel (a CCMP 128 bites blokkonként titkosít), valamint az üzenetcserék számával magyarázható. Az újrahitelesítési folyamat időtartama csökkenthető azáltal, hogy a mobil kliens és a hitelesítő szerver ideiglenesen letárolják a közös PMK-t, így nem szükséges ennek a kulcsnak az újragenerálása a folyamat során. Továbbá kimutatható, hogy a bázisállomások pufferének mérete, illetve az állomás puffer-kezelési algoritmusának intelligenciája jelentősen befolyásolja a cellaváltási és a TCP teljesítményt. Az L2-es roaming, illetve a teljes forgalomkiesés időtartamának csökkentéséhez a tárgyalt részfolyamatok optimalizálása szükséges. Erre a problémára a jövőben a - jelenleg tervezetként létező - IEEE 802.11r szabvány adhat megoldást.

7. Irodalom

[1] Zoltán Gál, Andrea Karsai, Péter Orosz: „Evaluation of IPv6 Services in Mobile WiFi Environment”, *Selected Papers of Info-Communication-Technology*, Volume LX., 2005., pp 47-54.

[2] Wi-Fi Protected Access Data Encryption and Integrity: http://www.microsoft.com/technet/community/columns/cableguy/cg1104.mspx

[3] Securing Wi-Fi Wireless Networks with Today's Technologies: http://www.wi-fi.org/files/uploaded_files/wp_4_Securing%20Wireless%20Networks_2-6-03.pdf
[4] Scott Fluhrer, Itsik Mantin, Adi shamir: „Weakness in the Key Scheduling Algorithm of RC4", http://www.crypto.com/papers/others/rc4_ksaproc.pdf
[5] Orosz Péter, Sztrik János, Kim Che Song: „Központosított EAP alapú hitelesítés vezeték nélküli hálózatokban", Informatika a felsőoktatásban 2005. konferencia