Vezeték nélküli hálózatok

Számítástechnika tanár szak
Rendszertechnika II.
gyakorlat

Vezeték nélküli adatátvitel

- Vezeték nélküli átvitelt használó eszközök
  - Kis hatótávolságú adóvevők
  - Kis energiafogyasztás
  - Kis helyigény
- Jól használható megoldás
  - Mobiltelefonokban
  - Kéziszámítógépekben
  - Notebookokban
  - Fejhallgatókban
  - Távirányítókban
  - Nyomtatókban

IrDA

- IrDA (Infrared Data Association)
  - átvitel fény segítségével
  - hatótávolság: kb. 5-10 méter
  - kis teljesítményű verziók hatótávolsága kb. 20 cm
  - adatátviteli sebesség: akár 4 Mbit/s (max.: 1 méter)
  - rádiófrekvenciás zavarásra érzéketlen
  - Kizárólag akadálymentes környezetben használható
  - Csak pont-pont összeköttetésre használható

Bluetooth

- 1998 - IBM, Intel, Nokia, Ericsson, Toshiba
- átvitel rádióhullámok segítségével
  - nem igényel "rálátást"
  - Maximális átviteli sebesség 1 Mbit/s
- frekvenciasáv: 2,4 GHz
  - 2.402GHz - 2.480GHz
  - 79 vivőfrekvencia (1 MHz-es csatornaosztás)
  - 1600 (ál)véletlenszerű frekvenciaugrás másodpercenként
- Mester - szolga (Master - Slave) viszony
  - Időosztásos duplexelés
    - Mester: minden páratlan időrésben adhat
    - Szolga: minden páros időrésben adhat
  - 1 mesterhez maximum 7 szolga tartozhat egyszerre

Bluetooth csomagok

- 1, 3 vagy 5 egymás utáni időrést foglalhatnak el
  - egy időrés 1/1600 = 625μs
- csomagok felépítése
  - Hozzáférési mód (Access Code): 68/72 bit
    - időszinkronizálás, keresés, tudakozódás, felderítés
  - Fejrész (Header): 54 bit
    - csomagazonosítás, csomagszámozás (csomagok újrarendezéséhez), szolga címe, hibaellenőrző bitek
  - Adatrész (Payload): 0 … 2745 bit
    - beszédbitek, adatbitek vagy mindkettő

Bluetooth frekvenciák és teljesítmények

- Frekvenciaugrások
  - 1600 frekvenciaugrás másodpercenként
- Adaptív frekvenciaugrások
  - Bluetooth 1.2 szabványtól kezdve
  - A 802.11b és 802.11g szabványokkal való interferencia elkerülése érdekében
  - Közös frekvenciák kizárása
  - Egy kérdés-válasz alatt a mester és a szolga azonos frekvenciát használ → 800 ugrás másodpercenként
- Eszközök teljesítménye
  - alacsony energiaigény
  - alacsony kimenő teljesítmény
    - Class1: 100 mW
    - Class2: 2,5 mW
    - Class3: 1 mW
  - Élettani hatása elhanyagolható

Bluetooth átviteli módok

- SCO (Szinkron, kapcsolat alapú összeköttetés)
  - szimmetrikus pont-pont összeköttetés (Master-Slave)
  - meghatározott időközönként foglal a mester egy időrést
  - 64 kbit/s mindkét irányban (ált. beszédátvitelhez)
  - nincs csomagismétlés
  - egy mester maximum 3 párhuzamos kapcsolatot tud fenntartani
- ACL (Aszinkron, kapcsolat nélküli összeköttetés)
  - aszimmetrikus pont- több pont közötti összeköttetés
  - azokban az időrésekben használható ahol nincs SCO kapcsolat
  - egyszerre egy aktív ACL kapcsolat lehetséges
  - általában alkalmazzák a csomagok újraküldését
  - maximális átviteli sebesség: 732 kbit/s

Bluetooth állapotok

- Nyugalmi állapot (Standby)
  - alacsony energiafogyasztás
  - csak az óra működik, nincs élő kapcsolat
- Lekérdezés és keresés (Inquiry and Page)
  - Lekérdezés (a környezetben található eszközök detektálása)
  - Keresés - a kapcsolat felépítése az adott eszközzel
- Kapcsolati állapot
  - Aktív mód - ha az eszköz ténylegesen kommunikál
  - Sniff mód
    - a slave csak meghatározott időrésekben figyel
    - a mester csak ezekben az időrésekben üzenhet a szolgának
  - Tartás (Hold) mód
    - a mesterrel egyeztetett ideig a szolga csak az SCO csomagokra figyel
    - az idő lejárta után a szolga feléled, újraszinkronizál és veszi a csomagokat
  - Park mód
    - egy pikohálózatban akár 255 eszköz is lehet virtuálisan
    - ha már van 7 aktív szolga vagy 1 aktív mester, akkor kerülhet park állapotba az eszköz

Bluetooth biztonság

- Alapvető biztonsági elemek
  - 48 bites egyedi eszközcím
  - 128 bites saját azonosító kulcs
  - 8-128 bites saját kódoló kulcs
  - Az eszköz által generált, gyakran változó véletlen szám
- Bluetooth biztonsági szintek
  - Nincsenek biztonsági megkötések
  - Szolgáltatás szintű biztonsági intézkedések
  - Kapcsolat szintű biztonsági intézkedések
- Kulcskezelés
  - Összekötő kulcsok (Link keys)
  - Titkosító kulcsok

Bluetooth összekötő kulcsok

- Kombinációs kulcs (combination key)
  - használatáról az eszközök döntenek az inicializációs folyamat során
  - A két eszközben egyszerre jön létre egy algoritmus (E21) alapján
    - véletlenszám generálás
    - a véletlenszám kombinálása a saját eszközcímükkel
    - véletlenszámok kicserélése, közös kombinációs kulcs kiszámítása
- Egység kulcs (unit key)
  - az eszköz első használatakor jön létre az E21 kulcsgeneráló algoritmus alapján
  - Két eszköz használhatja az egyik egység kulcsot összekötő kulcsként
- Elsődleges kulcs (master key)
  - A mester által generál ideiglenes kulcs
  - Mindenki egy kivonatot generál az aktuális összekötő kulccsal
  - A mester bitenként XOR-ozza a kivonatot a generált elsődleges kulccsal
  - A szolgák szintén XOR művelettel visszafejtik ezt a kivonat alapján
  - Minden fél alkalmazza az új összekötő kulcsot
- Inicializáló kulcs (initialization key)
  - Amikor nincs mester - szolga viszony
  - Inicializációkor mindkét eszközben meg kell adni egy PIN kódot
  - A kulcs az E22 algoritmussal a PIN kód, egy 128 bites véletlen szám és a kezdeményező eszköz eszközcímének kombinálásával jön létre
  - A kulcs egyszer használatos

Bluetooth titkosítás

- Titkosítási módok
  - egység- vagy kombinációs kulcs esetén az adatátvitel nincs titkosítva
  - Elsődleges kulcs használata esetén
    - nincs titkosítás
    - az adatátvitel nem titkosított, csak a belső adatforgalom
    - minden adatforgalom az elsődleges kulccsal kódolt
- Authentikáció
  - Kérdés-felelet formájában szimmetrikus kulcsokkal
    - Az azonosítást végző fél küld egy véletlen számot a kérelmezőnek
    - Mindkét fél alkalmazza az E1 algoritmust a véletlen szám, az aktuális összekötő kulcs és a kérelmező eszközcímének értékeire
    - A kiszámolt digitálisan aláírt választ (SRES) a kérelmező visszaküldi
    - Az azonosítást végző összehasonlítja az SRES értékét az általa kiszámolttal
      - Ha egyezik akkor sikeres az authentikáció
      - Ha nem egyezik a két érték akkor duplázódó várakozás után tehető újabb kísérlet

Bluetooth kapcsolódás

- A kapcsolatfelvétel engedélyezésének módja
  - Mindenki számára engedélyezett
  - A felhasználó maga dönti el, hogy mely kapcsolatokat engedélyez
- Felhasználó által jóváhagyott kapcsolat felépítése
  - Authorizáció (felhasználói jóváhagyás)
  - Authentikáció
  - Összekapcsolás
    - közös kulcs (PIN) alkalmazásával
      - Mindkét oldalon azonosan kell bevinni
  - Titkosítás

Bluetooth biztonsági problémák

- A titkosításnál alkalmazott E0 algoritmus elméletileg feltörhető egy bonyolult matematikai eljárással
  - ha a kulcssorozat hosszabb mint az E0-nál használt legrövidebb regiszter
  - A több GHz-en működő eszközben a kódgeneráló algoritmus kimenetéhez kellene hozzáférni frissítés közben
- PIN problémák
  - Egyetlen titkos része az inicializáló kulcsnak
  - Négy számjegy esetén szóba jöhet a brute force módszer
  - (Humán tényezők)
  - Az E22 algoritmus ismeretében kiszámolható az inicializáló kód
- Az egység kulcsok problémája
  - A és B eszköz A egység kulcsát használja a kommunikációhoz
  - C csatlakozik A-hoz, megkapja annak egységkulcsát
  - C egység B eszközcímének meghamisításával lehallgathatja A-B kommunikációját

Vezeték nélküli hálózatok WLAN

- 2000 környékén terjedt el széles körben
- Manapság bizonyos esetekben alternatívája a vezetékes hálózatoknak
- Alacsony ár, egyszerű kiépíthetőség
- Mobil felhasználási lehetőségek
- Széles körű felhasználási lehetőségek
- Hatósugár
  - Épületeken belül akár 100 méter
  - Épületeken kívül akár 300 méter
  - Hatósugár tovább növelhető. Antennák, ismétlők

WLAN szabványok - Home RF

- Legkorábbi szabvány
- Működési frekvencia: 2,4 GHz
- Moduláció: FHSS (Frequency Hopping Spread Spectrum)
- 15 interferencia mentes csatorna
- Zavarásokra kevésbé érzékeny
- Maximális sebesség
  - 1,6 Mbit/s (v 1.2 - 2001-ig)
  - 10 Mbit/s (v 2.0 - 2001 végétől)
- A 802.11b szabvány a 2.0-ás verzió megjelenésekor már népszerűbb volt …

WLAN szabványok
IEEE 802.11b

- Működési frekvencia: 2,4 GHz
- Nem harmonizált, szabadon felhasználható sáv
- Moduláció: DSSS (Direct Sequence Spread Spectrum)
- Maximális sebesség: 11 Mbit/s
  - távolság miatti sebesség visszaesések
    - 5,5 Mbit/s
    - 2 Mbit/s
    - 1 Mbit/s
- 3(+1) interferencia mentes csatorna
- Hatótávolság: akár 100 méter épületen belül
- Bluetooth eszközök, vezeték nélküli telefonok, mikrohullámú sütők esetleg zavarhatják az átvitelt

IEEE 802.11b csatornakiosztás

Csatorna	Vivőfrekvencia	Frekvenciasáv	Amerika	Európa	Izrael	Kína	Japán
1	2412 MHz	2401-2423 MHz	X	X	-	X	X
2	2417 MHz	2406-2428 MHz	X	X	-	X	X
3	2422 MHz	2411-2433 MHz	X	X	X	X	X
4	2427 MHz	2416-2438 MHz	X	X	X	X	X
5	2432 MHz	2421-2443 MHz	X	X	X	X	X
6	2437 MHz	2426-2448 MHz	X	X	X	X	X
7	2442 MHz	2431-2453 MHz	X	X	X	X	X
8	2447 MHz	2436-2458 MHz	X	X	X	X	X
9	2452 MHz	2441-2463 MHz	X	X	X	X	X
10	2457 MHz	2446-2468 MHz	X	X	-	X	X
11	2462 MHz	2451-2473 MHz	X	X	-	X	X
12	2467 MHz	2456-2478 MHz	-	X	-	-	X
13	2472 MHz	2461-2483 MHz	-	X	-	-	X
14	2484 MHz	2473-2495 MHz	-	-	-	-	X

WLAN szabványok
IEEE 802.11a

- Bemutatkozás: 2001 végén
- Működési frekvencia: 5 GHz
- Moduláció: OFDM (Orthogonal Frequency Division Multiplexing)
- Maximális sebesség: 54 Mbit/s
- 12 interferencia mentes csatorna
- Nem kompatibilis visszafelé a 802.11b szabvánnyal
- A nagyobb frekvenciás jelek nehezebben hatolnak át falakon, épületen belüli felhasználást korlátozza
  - Épületen belül jellemzően a max. áthidalható távolság 30m

IEEE 802.11a csatornakiosztás

Csatorna	Vivőfrekvencia	Frekvenciasáv	Amerika	Japán	Szingapúr	Taiwan
34	5170 MHz	5160-5180 MHz	-	X	-	-
36	5180 MHz	5170-5190 MHz	X	-	X	-
38	5190 MHz	5180-5200 MHz	-	X	-	-
40	5200 MHz	5190-5210 MHz	X	-	X	-
42	5210 MHz	5200-5220 MHz	-	X	-	-
44	5220 MHz	5210-5230 MHz	X	-	X	-
46	5230 MHz	5220-5240 MHz	-	X	-	-
48	5240 MHz	5230-5250 MHz	X	-	X	-
52	5260 MHz	5250-5270 MHz	X	-	-	X
56	5280 MHz	5270-5290 MHz	X	-	-	X
60	5300 MHz	5290-5310 MHz	X	-	-	X
64	5320 MHz	5310-5330 MHz	X	-	-	X
149	5745 MHz	5735-5755 MHz	-	-	-	-
153	5765 MHz	5755-5775 MHz	-	-	-	-
157	5785 MHz	5775-5795 MHz	-	-	-	-
161	5805 MHz	5795-5815 MHz	-	-	-	-

WLAN szabványok
IEEE 802.11g

- 2003-ban elfogadott szabvány
- Működési frekvencia: 2,4 GHz
- Moduláció: OFDM (Orthogonal Frequency Division Multiplexing)
- Maximális sebesség: 54 Mbit/s
- 3 interferencia mentes csatorna
- Kompatibilis visszafelé a 802.11b szabvánnyal
- Bluetooth eszközök, vezeték nélküli telefonok, mikrohullámú sütők esetleg zavarhatják az átvitelt

IEEE 802.11g csatornakiosztás

Csatorna	Vivőfrekvencia	Frekvenciasáv	Amerika	Európa	Izrael	Kína	Japán
1	2412 MHz	2401-2423 MHz	X	X	-	X	X
2	2417 MHz	2406-2428 MHz	X	X	-	X	X
3	2422 MHz	2411-2433 MHz	X	X	X	X	X
4	2427 MHz	2416-2438 MHz	X	X	X	X	X
5	2432 MHz	2421-2443 MHz	X	X	X	X	X
6	2437 MHz	2426-2448 MHz	X	X	X	X	X
7	2442 MHz	2431-2453 MHz	X	X	X	X	X
8	2447 MHz	2436-2458 MHz	X	X	X	X	X
9	2452 MHz	2441-2463 MHz	X	X	X	X	X
10	2457 MHz	2446-2468 MHz	X	X	-	X	X
11	2462 MHz	2451-2473 MHz	X	X	-	X	X
12	2467 MHz	2456-2478 MHz	-	X	-	-	X
13	2472 MHz	2461-2483 MHz	-	X	-	-	X
14	2484 MHz	2473-2495 MHz	-	-	-	-	X

2,4 GHz vs. 5 GHz

- Felhasználás földrajzi helye
- Teljesítőképesség
  - 802.11a - 12 db. nem átlapolódó 20 MHz széles csatorna
  - 802.11b/g - 3 db. független csatorna, 80 MHz teljes sávszélesség
- Épületméret
- Rádiófrekvenciás interferencia
- Kompatibilitás
- Biztonság (elérhetőség épületen kívül)

WLAN eszközök - Rádió modem

- Rádió modem
  - Feladatok
    - moduláció, jeltovábbítás
    - jelek vétele, demoduláció
  - Részei: antenna, erősítők, frekvencia szintézerek és szűrők
  - Főbb jellemzői: frekvenciasáv, jelzéssebesség, moduláció, kimenő teljesítmény
- MAC (Message Authentication Code) kontroller
  - Feladatok
    - csatorna hozzáférés
      - TDMA - időosztásos többszörös elérés
      - CSMA/CA - vivő érzékelő többszörös elérés / ütközés elkerülés
      - MAC lekérdezés
    - hálózatmenedzsment

Átviteli jellemzők

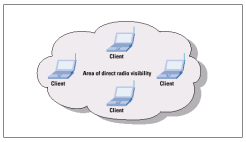
- Adóteljesítmény
- Érzékenység
- Csillapítás
- Jel/zaj viszony
- Elhalkulás (fading)
- Zavarások

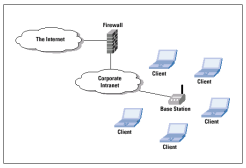
WLAN hardver elemek

- Rádiófrekvenciás hálózati kártyák
  - Fizikai réteg: 802.11a, 802.11b/g, 802.11a/b/g
  - Csatlakoztatás: PCI, mini PCI, PCMCIA, CF, USB
- Hozzáférési pontok
  - Rádiófrekvenciás + vezetékes hálózati kártya
  - Általában HTTP protokollon keresztül konfigurálható
- WLAN Routerek
  - Többportos Ethernet router + hozzáférési pont
  - Jellemző szolgáltatások: NAT, DHCP, Firewall, Repeater
- Ismétlők (repeater)
  - Hatósugár kiterjesztése jelformázással és erősítéssel
  - Összes keret újraküldése azonos csatornán, duplázódó forgalom
- Antennák
  - Körsugárzó vagy irányított antennák
  - Csatlakoztatási lehetőségek az eszközökön
  - Előírt kimenő teljesítmény

WLAN topológiák

- Ad-hoc hálózatok
  - két vagy több kliens összekapcsolása egymással
  - nincs kiemelt elem
- Menedzselt vagy infrastrukturális hálózatok
  - a kliensek egy kiemelt elemen (AP) keresztül kapcsolódnak
  - A forgalom szűk keresztmetszete lehet az AP
  - Lehetőség van hitelesítésre, forgalom szűrésre, a hozzáférések kontrollálására





http://www.isoc.org

WLAN biztonsági problémák

- Forgalomfigyelés
  - Titkosítatlan forgalom könnyen figyelhető (AirMagnet, AiroPeek)
  - Titkosított forgalom is lehallgatható és rögzíthető
  - Nem szükséges a fizikai jelenlét
- Jogosulatlan hozzáférés
  - Alapértelmezésben használt eszközök veszélyei
  - Engedély nélküli hozzáférési pontok telepítése későbbi támadási pontként
- ARP támadások (nem csak WLAN esetén)
  - ARP (Address Resolution Protocoll): IP-hez MAC címet rendel
  - Érvényes IP címhez hamis MAC cím adható
    - Az adott IP-re küldött csomagok a hamis MAC felé továbbítódnak
  - Megoldás lehet a Secure ARP

WLAN biztonsági problémák

- Szolgáltatásmegtagadás (DoS)
  - Legegyszerűbb támadási forma, számolni kell a lehetőséggel
    - Másodlagos csatornák üzemeltetése
  - Elárasztás (használhatatlan csomagokkal)
  - Elnyomás (nagyobb teljesítményű rádiójellel)
  - Véletlen interferenciák
  - Kívülről érkező rádiójelek elleni védelem
    - Adók teljesítményének hangolás, a jel épületen belül tartása
    - Az épület árnyékolása (fémfólia alapú ablakszigetelés, fémszórt ablaküveg, fém alapú festékek, stb.)

WLAN titkosítás - WEP

- WEP: Wired Equivalent Privacy
- MAC rétegben implementált opcionális titkosítási és hitelesítési szabvány
- Szimmetrikus kulcsú eljárás
- A keretek törzsének és CRC részének RC4 titkosítására szolgál
- A titkosítás folyamata
  - kulcssorozat előállítása
    - felhasználó által megadott WEP kulcsból
    - 24 bites, minden keret küldése előtt véletlenszerűen változó inicializáló vektorból (IV)
    - Az adatkeret és a ICV érték kódolása a kulcssorozattal (XOR)
- Az átvitel sértetlensége
  - Integritás ellenőrző érték, ICV (Integrity Check Value)
    - A vevő is kiszámítja a kapott adatokból és összehasonlítja az érkezett ICV-vel

A WEP problémái

- Közös, statikus jellegű, nehezen változtatható kulcsok
  - Ritkán kerül megváltoztatásra (akár évek is)
- Rövid (24 bites) inicializáló vektorok
  - Több adatcsomagnál előfordulhatnak azonos IV-k
  - Azonos kulcssorozattel rendelkező keretek
    - Keretek közös értékei (kulcssorozat vagy WEP kulcs) meghatározható
- Csak minimális biztonság elérésének céljából alkalmazható
  - Jellemzően otthoni hálózatokban megfelelő lehet
  - Sokkal jobb megoldás a nyílt hálózatoknál …

WLAN titkosítás - WPA

- WPA (Wi-Fi Protocol Access)
- A WEP továbbfejlesztése
  - Periodikusan változó titkosító kulcsok
    - Kulcsok változtatása a TKIP segítségével
  - Kölcsönös hitelesítési lehetőségek
  - Autentikációs szerverek (RADIUS) bevonásának lehetősége
  - 48 bites IV
  - Sértetlenség ellenőrzés
    - 8 bites MIC (Message Integrity Code)
    - 24 bites ICV
- Átmeneti megoldás
  - Végleges megoldás 802.11i szabványban

WLAN titkosítás - TKIP

- TKIP (Temporal Key Integrity Protocol)
- A WEP protokol esetében megoldja a kulcsok újrafelhasználásából adódó gondokat
  - Számos eszköz új firmware-el átalakítható
  - Megmarad a WEP kompatibilitás
- A TKIP folyamat
  - 128 bites ideiglenes kulcs megosztás a kliens és az AP között
  - Az ideiglenes kulcs és a kliens MAC címének egyesítése
  - 16 bájtos IV hozzáadása
- Az ideiglenes kulcs 10.000 csomagonként változik

WLAN titkosítás - AEP

- AEP (Advanced Encryption Standard)
- Az IEEE 802.11i szabvány tartalmazza a TKIP mellett
- RC4 helyett Rine Dale titkosító algoritmus
- 128, 192, 256 bites kulcsok
- Visszafelé kompatibilis a WPA protokollal
- Hátrányai:
  - nagyobb számítási teljesítményigény
  - új hardverelemek szükségesek (kódolás gyorsító processzorok)

WLAN hitelesítés - WEP

- A kliens hitelesítés iránti kérelmet küld
- A hozzáférési pont válaszként egy speciális "felkérő szöveget" küld a kliens felé
- A kliens a "felkérő szöveget" titkosítja a közös WEP kulccsal és visszaküldi az AP-nek
- Az AP a WEP kulccsal visszafejti az üzenetet és összhasonlítja az által küldöttel
- Ha küldött és a visszafejtett szöveg megegyezik a hozzáférési pont hitelesíti a klienst

WLAN hitelesítés - IEEE 802.1x

- EAP (Extensible Authentication Protocol) használata
- A kliens hitelesítés iránti kérelmet küld
- Az AP egy azonosító iránti kérést tartalmazó EAP üzenettel válaszol.
- A kliens az AP egyetlen nyitott portján továbbítja az azonosítást tartalmazó választ a hitelesítést végző szerverhez
  - Minden más portot lezárva tart a kliens előtt
- A hitelesítő szerver elutasító vagy elfogadó üzenetet küld a bázisállomásnak
- A bázisállomás sikeres hitelesítést jelző AEP csomagot küld a kliensnek
- Ha minden sikeres volt, a bázisállomás elérhetővé teszi a további engedélyezett portokat is a kliensnek

WLAN beállítások - SSID

- SSID (Service Set IDentifier)
- Az AP olyan jelzőkereteket sugároznak amik tartalmazzák az SSID-t
- Csatlakozás akkor történhet ha az AP SSID-je egyezik a kliensen beállított SSID-vel
- SSID elrejtésének lehetősége
  - Az SSID azonosító a kommunikáció során titkosítás nélküli
  - Kliens eszközök csatlakozási kérelmének lehallgatása
- Nem eredményezi a biztonság jelentős növekedését

WLAN beállítások - MAC filter

- A hozzáférési pontok általában támogatják a MAC szűrést
- Az AP megvizsgálja a beérkező kereteket
  - Ha a forrás MAC címe engedélyezve van továbbítja a keretet
  - Ha a forrás MAC címe nincs engedélyezve elutasítja a keretet
- A MAC címek az átvitel során nem titkosítottak
- Egy megszerzett MAC cím beállítható más eszközökön is, így álcázhatja magát a támadó
- Nehézkes a MAC címek adatbázisának kezelése is

A WLAN biztonság fokozása

- A WLAN felhasználóinak elhelyezése a tűzfalon kívül, DMZ-ben
- Hatékony titkosítás alkalmazása
- A firmware-ek rendszeres frissítése
- A hozzáférési pontok fizikai rögzítése, elrejtése, reset gomb (!)
- Elérés tiltása üzemszünet esetén
- Bonyolult jelszavak megadása az AP-khez
- SSID broadcast tiltása
- Rádióhullámok terjedésének szabályozása
- Kliensek védelme személyes tűzfallal
- Bázisállomások forgalmának monitorozása, csaló AP-k kizárása
- Telepítések, fejlesztések felügyelete
- Hozzáférési pontok és kliensek MAC címének nyilvántartása