

**XXXI. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2013. április 16-18.
Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar**

**VEZETÉK NÉLKÜLI ELEKTRONIKUS
BIZTONSÁGTECHNIKAI ESZKÖZÖK ÉS RENDSZEREK
FUNKCIÓNAK, VALAMINT ALKALMAZHATÓSÁGUK
KORLÁTAINAK VIZSGÁLATA**

Jelige: *Alfa*

Dolgozat lezárásának időpontja: 2012, május

Tartalom

Tartalom	2
Bevezetés	4
1 Elektronikus biztonságtechnikai rendszerek	7
1.1 Elektronikus eszközök a biztonságtechnikában	8
1.1.1 Területvédelmi eszközök, érzékelők	8
1.1.2 Felületvédelmi eszközök, érzékelők.....	11
1.2 Elektronikus biztonságtechnikai rendszerek	17
1.2.1 Behatolásjelző rendszerek	17
1.2.2 Beléptető rendszerek.....	18
1.2.3 Távfelügyeleti rendszerek.....	21
1.2.4 CCTV rendszer	21
1.2.5 Integrált felügyeleti rendszerek	23
2 Elektronikus biztonságtechnikai rendszerek rádiófrekvenciás kommunikációs platformjai	25
2.1 Hagyományos rádiófrekvenciás átvitel alapvető tulajdonságai.....	27
2.1.1 Abszorpció.....	27
2.1.2 Reflexió	28
2.1.3 Polarizáció	28
2.1.4 Interferencia.....	29
2.2 A GSM technológia biztonsága.....	30
2.3 Bluetooth	32
2.3.1 A Bluetooth biztonságra	33
2.3.2 Bluetooth biztonságának gyenge pontjai	36
2.4 Lézeres adatátvitel	37
3 Vezeték nélküli IP hálózatok biztonsági kérdései	39

3.1 WLAN hálózatok biztonságos kialakítása.....	40
3.1.1 Illetéktelen hozzáférés	40
3.1.2 Hozzáférési pontok felügyelete	41
3.1.3 Titkosítás és autentikáció.....	42
3.1.4 A vezeték nélküli hálózatok használatának szabályozása	43
3.1.5 Behatolás érzékelés és megelőzés	44
3.2 Támadási módszerek	44
3.3 Támadási formák	45
3.3.1 Az aktív támadások általános formája.....	45
3.3.2 Visszaélés a MAC-címmel	46
3.3.3 Közbeékelés támadás (Man-in-the-Middle Attack).....	46
3.3.4 Lehallgatás.....	47
3.4 A vezeték nélküli hálózatok biztonsága	47
3.4.1 Forgalommonitorozás.....	48
3.4.2 Jogosulatlan hozzáférés	49
3.5 Az IEEE 802.11x szabványai	53
3.5.1 IEEE 802.11a.....	53
3.5.2 IEEE 802.11b	53
3.5.3 IEEE 802.11g	54
3.5.4 IEEE 802.11i	55
3.5.5 IEEE 802.11n	55
Összefoglalás.....	57
Irodalomjegyzék	59
Rövidítésjegyzék	61

Bevezetés

A biztonságtechnikai rendszerek alkalmazása az utóbbi évek, évtizedek során az élet és vagyonbiztonságot fenyegető tényezők számának növekedése, valamint a kialakítás költségeinek csökkenése következtében egyre elterjedtebbé vált. A kormányzati, pénzügyi, kereskedelmi és ipari létesítmények mellett a magánszférában is fokozódó igény mutatkozik az adott környezetre optimális biztonsági koncepció kialakítására. A feladat azért komplex, mert egy valóban teljes körű védelmet nyújtó megoldáshoz a megfelelő technikai eszközök kiválasztása mellett nagy figyelmet kell fordítani a személyi biztonsági kockázatokra is, illetve az ezek alapján megalkotandó működést szabályozó belső intézkedésekre is. Ennek megfelelően integrált biztonsági megoldásokról, rendszerekről a fizikai¹, logikai² és humán³ biztonsági megoldások együttes alkalmazása esetén beszélhetünk.

A komolyabb képességekkel felruházott biztonságtechnikai rendszerek komplexitása sok esetben összemérhető a különböző ipari rendszerekével, azzal a különbséggel, hogy az ipari folyamatokra már hosszú idő óta léteznek bizonyíthatóan hatékony és széles körben elterjedt eljárások, míg a biztonságtechnika területén jóval kevesebb jól megalapozott eredmény áll rendelkezésre a rendszerek tervezése során.

Egyszerűen fogalmazva tökéletes biztonság nem létezik, mégis törekedni kell rá. Az optimális biztonság⁴ fölötti szinten helyezkedik el az a maradék kockázat, amivel minden esetben tudatosan számolni kell. Azaz be kell látnunk, hogy egyes veszélyekre egyáltalán nem, vagy csak részben tudunk felkészülni megfelelő védelmi megoldásokkal.

Amikor egy problémát egy máshol alkalmazott technológia, vagy eljárás segítségével oldunk meg, mindig figyelembe kell vennünk annak biztonsági kockázatait, mert az befolyásolni fogja rendszerünk használhatóságát, eredő biztonságát. Ez a technológia transzfer, azaz megoldás „kölcsonzés” szolgál dolgozatomban alapjául, amelynek alapvető célja, hogy a különböző vezeték nélküli technológiákra épülő vagyonvédelmi, tűzjelző, beléptető, épületautomatizálási és videó megfigyelő rendszerek (együttesen vezeték nélküli biztonságtechnikai berendezések), illetve azok elemei műszaki paramétereinek, valamint

¹ infrastruktúra védelem, beléptetés, tűzvédelem

² informatikai behatolás védelem, adatbiztonság

³ visszaélések, szándékos károkozás

⁴ amikor a befektetett erőforrások arányosak a kialakított védelem szintjével

működést befolyásoló tulajdonságainak vizsgálatán keresztül világítson rá azok alkalmazhatósági, különös tekintettel a rendszerek biztonságát, megbízhatóságát érintő kérdésekre.

Szükségesnek tartom megjegyezni, hogy az elektronikus biztonságtechnikai rendszereknél a „vezeték nélküliséget” elsősorban átviteltechnika és nem szenzortechnika vonatkozásában (kommunikációs csatorna) kívánom értelmezni.

Az első fejezetben olyan alapvető elektronikus biztonságtechnikai rendszerek kerülnek bemutatásra, amelyek elemei a komplex védelem kialakításában, a maradék kockázat csökkentésében jelentős szerepet játszanak. Az egyes elemek összekapcsolása, az általuk előállított információk továbbítása, valamint vezérlésük biztosítása során lehetőség van arra, hogy a vezetékes átviteli utakat vezeték nélküli megoldásokkal váltsuk ki, ezáltal minimálisra csökkentve a rendszer kialakításakor az objektumban végrehajtandó átalakítások szükségességét, a fizikai átviteli utak kiépítésének költségeit, fokozva a tervezés rugalmasságát, megteremtve egy későbbi, lényegesen gyorsabb és költséghatékonyabb átalakítás lehetőségét. Mivel az átviteli utak a tervezésnél a biztonsági szempontokat sokszor háttérbe szorítják a pénzügyi háttér korlátai, ezért az előkészítő fázisban alaposan meg kell vizsgálni, milyen megoldásokat választunk, akár jelentős kompromisszumok (ár-funkcionalitás, ár-megbízhatóság, ár-rugalmasság) árán is.

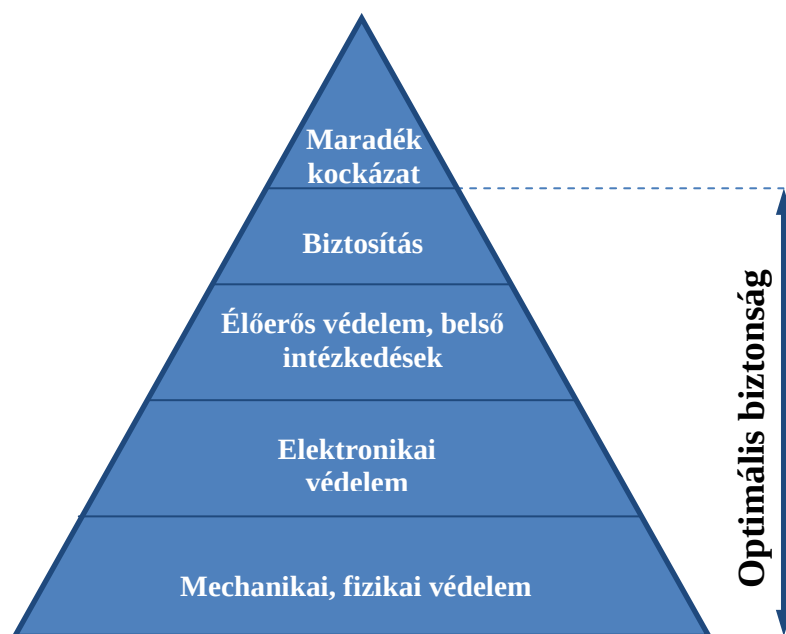
A második rész a klasszikus rádiófrekvenciás átviteli megoldások alapvető fizikai tulajdonságaival foglalkozik, amelynek keretében ismertetésre kerülnek a biztonságtechnikai rendszerek által elterjedten alkalmazott átviteltechnikai platformok frekvenciatartományaiban, a rádióhullámok terjedésével összefüggő jellemzők és anomáliák. Az abszorpció, reflexió, polarizáció és interferencia jelenségének bemutatását követően a GSM, Bluetooth és lézeres technológia biztonsági kérdései kerülnek összefoglalásra.

A harmadik fejezet az egyre elterjedtebben használatos IP alapú vezeték nélküli informatikai hálózatok biztonsági kérdései köré épül. Először a biztonságos rendszer kialakításához szükséges védelmi intézkedések, majd a támadási módokat és formákat követően a hálózati biztonság kérdései kerülnek tárgyalásra. A fejezet azon vezeték nélküli hálózatokat determináló szabványok bemutatásával zárul, amelyek alapját képezhetik a korszerű vezeték nélküli elektronikus biztonságtechnikai rendszerek kommunikációs platformjának.

A dolgozat elsősorban a tervezés során figyelembe veendő szempontokra és körülményekre, valamint azokra a rendszerek kialakításakor szóba jöhető vezeték nélküli kommunikációs megoldásokra (illetve biztonsági hiányosságaira) fókuszál, amelyek széles körben elterjedt szabványokon alapuló, kereskedelmi forgalomban hozzáférhető eszközrendszeren alapulnak. Nem célja a felmerülő problémákra konkrét válaszok keresése, hiszen azok mélyreható vizsgálata, illetve a szükséges megoldások kidolgozása egyesével is meghaladják egy ilyen dolgozat kereteit. Egy konkrét feladatra optimalizált vezeték nélküli elektronikus biztonságtechnikai rendszer kialakítása során a felmerülő anomáliákat a rendelkezésre álló tervezési alapadatok és peremfeltételek pontos ismeretében lehet csak megoldani.

1 Elektronikus biztonságtechnikai rendszerek

Az információs technológia és ezzel párhuzamosan az elektronikus eszközök gyors fejlődése a reakcióidő csökkenésén, valamint a védelem szintjének növekedésén keresztül biztosítja a maradék kockázat mérséklését, így utat nyit az integrált biztonságtechnikai rendszerek széleskörű alkalmazása terjedéséhez [1]. Az elektronikus biztonságtechnikai rendszerek helyét és szerepét az általános értelemben vett optimális biztonság fogalomkörében, valamint a maradék kockázat értelmezését az 1. ábra szemlélteti.



1. ábra: A komplex védelem értelmezése

Ahhoz, hogy be lehessen határolni azon eszközök körét, amelyek rendszerbe történő integrálásakor számolhatunk a vezeték nélküli technológiák átvételével, érdemes áttekinteni az alapvető elektronikus biztonságtechnikai rendszerek és berendezések körét. Az elektronikai védelem eszközeinek egyfajta csoportosítása a védendő terület jellege szerint történik, amely alapján megkülönböztetünk kültéri-, tér/terület-, felület/héj-, tárgy/vagyon- és személyvédelmi eszközöket.

1.1 Elektronikus eszközök a biztonságtechnikában [2]

Az elektronikai biztosítás sokrétű, folyamatosan bővülő és korszerűsödő eszközök, rendszerek alkalmazását jelenti, amelyek az egyszerű jelzéstovábbításon túl speciális képességeikkel képesek támogatni a megfogalmazott biztonsági célkitűzések megvalósulását.

Az elektronikai védelmi rendszerek fontos jellemzői, illetve alapvető követelményei a szuverenitás, a modularitás és a szabotázs elleni védelem képessége.

1.1.1 Területvédelmi eszközök, érzékelők

Ebbe a csoportba olyan – különböző fizikai jelenségeken alapuló – eszközök tartoznak, amelyek jelezni képesek adott terület, objektum, vagy épület „szuverenitását” illetéktelenek általi megsértését.

1. Hidraulikus lépésjelzők: földfelszín alá telepített, fagyálló folyadékkal töltött tömlőkből, érzékelőkből és ellenőrző egységekből felépülő kültéri érzékelő eszközök, melyek mára korszerűtlenné váltak. Bár telepítésük meglehetősen körülményes, jó minőségű anyagokat felhasználva, elektronikus érzékelővel kombinálva történő alkalmazásuk még ma is életképes, tartós megoldást jelenthet. Jóval egyszerűbb formája a kontaktszőnyeg, amely elektromos kapcsolókat tartalmaz, amelyek mechanikai nyomás hatására zárják a jelzőáramkört.
2. Mágneses térérzékelők: rejtetten, földfelszín alá telepített behatolás jelző rendszer, amely a földbe fektetett speciális elektromos kábel segítségével antennaként érzékeli az elektromágneses teret és az abban bekövetkező változásokat (fázis, amplitúdó). Ha a védett területen áthalad egy élőlény vagy egy jármű, az megváltoztatja a tér eloszlását, amit a rendszer érzékel és riasztást küld. Előnye, hogy a területen semmi nem látható, ami a védelmet elárulná, telepítése viszont körülményes és működési elvéből adódóan érzékeny a mozgó tereptárgyakra, fákra, elektromos vezetékekre, viharok által okozott elektromos jelenségekre.
3. Passzív mágneses térérzékelő: rejtett, intelligens érzékelő rendszer, amelyet szintén a földfelszín alatt kell elhelyezni. A rendszer alapja a mágneses anomália-érzékelés

(MAD⁵). A rendszer ferromágneses anyagok jelenlétét képes érzékelni, így minimalizálva a hamis jelzések kockázatát (állatok, erős szél, víz, hó stb.).

4. Infrasugaras eszközök, infrasorompók: „láthatatlan” botló drótként jelzik egy meghatározott területre adott útvonalon, vagy terepszakaszon történő behatolást. Ezek a berendezések egymással szemben felállított, vagy prizmákkal megfelelően irányítva, tetszőleges geometriában telepített adó-vevő párokból épülnek fel. Az adó által kibocsátott sugár nem folyamatos, hanem impulzus sorozatokból álló jel. A sugárnyaláb megszakítása jelzést generál. A hatótávolság a méteren belüli távolságtól egészen 150-200 méterig terjedhet. Az infrasorompók előnye, hogy működésük viszonylag védettnek tekinthető a környezeti- és időjárási jelenségekkel szemben.
5. Mikrohullámú érzékelők: a védendő terület, objektum határa mentén telepített jelzőrendszer. Működése azon alapul, hogy az egymással szemben felállított adó és vevő egységek között kialakuló mikrohullámú tér állapotát a behatoló személy vagy tárgy megváltoztatja. Ezt a változást érzékelve a vevő riasztó jelzést generál. Általában a radarokhoz hasonlóan doppler, illetve reflexiós elven működhetnek. A doppler elvűnél egy meghatározott pontból hullámforrást irányítunk a megfigyelendő irányba. A céltárgy közeledésekor annak a sugárforrás irányára eső sebességkomponens nagyságának ütemében növekszik a visszavert hullám frekvenciája, illetve ha távolodik, a sebességével arányosan csökken, amit a sugárzó irányában telepített vevő (létezhet más geometriai elrendezés is, ilyenkor mindig a vevő irányába eső sebességkomponens nagyságára lesz érzékeny a rendszer). A reflexiós elv alkalmazása esetén a közvetlen és a földről, vagy más reflektáló felületről/felületekről érkező jelek a vevő detektorán fázishelyesen összegződnek. A területre/térbe bekerülő „idegen test” megváltoztatja a reflexiós viszonyokat, ami az interferencia megváltozását, azaz jelszint változást eredményez a vevő bemenetén. Az érzékelők működési frekvencia tartománya 9-10 GHz. Az ilyen egyszerűen hálózatba fűzhető és távfelügyelhető eszközök előnye, hogy a támadó nehezebben tudja hatástalanítani, megtevesztetni őket, mint a passzív infravörös (PIR⁶) elvű szenzorokat, hátránya viszont a megnövekedett telepítési (drágább érzékelők) és üzemeltetési költség (nagyobb fogyasztás). Az ilyen eszközök karakterisztikája kevésbé variálható, ugyanakkor bizonyos feltételek teljesülése mellett „átlátnak” akár a falon is.

⁵ **M**agnetic **A**nomal **D**etection

⁶ **P**assive **I**nfra **R**ed

6. Ultrahangos érzékelők: szintén doppler elven működnek, a 25-40 kHz-es frekvencia tartományban. Előnyük, hogy egyszerű és olcsó alkatrészekből épülnek fel, hátrányuk viszont a zavarérzékenység. Működésük kívülről blokkolható, karakterisztikájuk szűk tartományban variálható és érzéketlenek a radiális irányra merőleges mozgásra, ugyanakkor „áthallanak” a falon (ez rejtettség szempontjából lehet előny, de zavarás szempontjából mindenképpen hátrány).
7. PIR: az emberi test hőmérsékleti sugárzását érzékelő, passzív eszköz. A környezetünkben minden tárgynak van valamilyen mértékű infravörös energia kibocsátása. Ha ezeket az infravörös hullámokat egy pontba fókuszáljuk és ebben a fókuszpontban egy piroelektronikus érzékelőt helyezünk el, a környezet hőtépképének megfelelően kialakul egy állandó értékű nyugalmi áram. Ha az érzékelő környezetében kisugárzott infravörös energiában hirtelen változás történik, az érzékelőn átfolyó áram értéke is megváltozik. Ezt a változást egy megfelelő jelfeldolgozó áramkör kiértékeli és kiadja a riasztás jelzést. A hőtépkép változásának oka lehet, ha megjelenik egy magasabb hőmérsékletű tárgy (gépjármű), vagy ember, illetve ha „kitakarásra kerül” egy magasabb hősugárzású tárgy, vagy irány. A külső zavaró hősugaraktól optikai szűrőkkel lehet védekezni. Típus szerint az eszköz lehet kitakarás védett, DSP⁷ processzoros, duál, „maga alá látó”, kisállat védett. Alkalmazott karakterisztika (látószög) szerint függöny, folyosó, normál (85-90°), 120-180°, mennyezeti (360°) és kültéri érzékelőket különböztetünk meg. A PIR hátránya, hogy becsapható (pl. lassú mozgás), és zavarérzékeny. Elhelyezésnél törekedni kell arra, hogy ne érje a Nap sugárzása.
8. Kombinált mozgásérzékelők: egy tokon belül tartalmazznak egy passzív infravörös és egy mikrohullámú, vagy ultrahangos doppler detektort. A kombinált mozgásérzékelők csak akkor generálnak riasztást, ha mind a két komponens egyidejűleg jelez, ezáltal csökkentve a téves riasztás kockázatát. Működési sebességüket a passzív infra szenzor „lomhasága” szabja meg. Megfelelő feldolgozó elektronika alkalmazásával – a PIR-hez hasonlóan – elérhető a mozgás irányának és sebességének érzékelése, amiből következtetni lehet annak valódiságára.

Ezek az érzékelők többnyire nem egyedileg, hanem egy, a közelben telepített központi vezérlőhöz csatlakoztatva, rendszerbe integrálva kerülnek alkalmazásra. A központ és végpontok viszonylatában jelentős adatforgalmazásra nem lehet számítani, hiszen a vezérlő

⁷ Digital Signal Processing – digitális jelfeldolgozás

által meghatározott időnként lefuttatott ellenőrzést (pl: szabotázs érzékelése), vagy a szenzor által küldött állapotjelentést leszámítva (pl: akkumulátor feszültség jelzése), információ akkor keletkezik, ha az érzékelő „rendellenességet” (területsértést) tapasztal. A továbbított adatok sebessége csekély, hiszen az információ ilyen érzékelők esetében mindössze annyi, hogy behatolás történt. Ennek továbbításához extrém alacsony sávszélességű (alacsony frekvencián üzemelő) csatorna is elegendő, ami analóg jelzésátvitel mellett is biztosítja a megfelelő illesztést, ugyanakkor digitális áramköri elemek alkalmazásával lehetőség nyílik nagy redundanciával rendelkező, robusztus kódolást és modulációt alkalmazó megbízható, zavarvédett rádiófrekvenciás interfész kialakítására is.

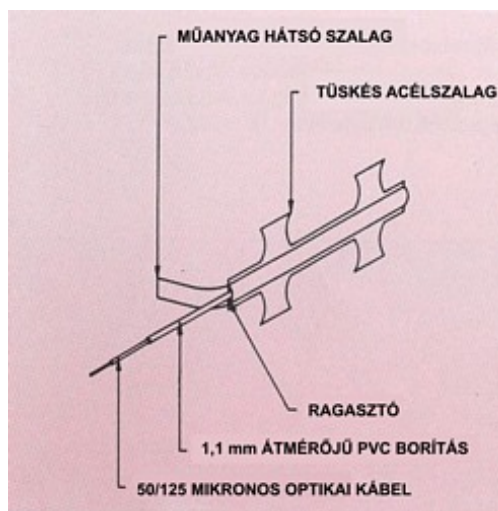
Autonom működésű érzékelők (integrált feldolgozó processzor), illetve vezérlő – távfelügyeleti központ viszonylatában az áthidalandó távolságtól függően létezhetnek a szabad felhasználású sávokban működő RH, URH és mikrohullámú kommunikációs eszközök is, ugyanakkor ha nem szempont a más rendszerektől teljesen független üzemeltetés, elterjedten alkalmazott megoldásként lehetőség van GSM⁸ modulok használatára, amelyek riasztás esetén hang, vagy szöveges üzenet hívást kezdeményeznek az előre megadott előfizetői számokra (tulajdonos, távfelügyeleti szolgáltató, biztonsági szolgálat, rendőrség stb.). Ennek előnye, hogy a hatótávolság bármekkora lehet, hiszen az információ továbbítása a mobiltelefon szolgáltatók cellás rendszerén keresztül történik. Az ilyen rendszerek elérhetőségét, megbízhatóságát és biztonságát alapvetően a mobiltelefon hálózatok tulajdonságai határozzák meg.

1.1.2 Felületvédelmi eszközök, érzékelők

1. Érzékelő kábeles rendszerek: olyan kerítésvédelmi rendszerek, melyek érzékelő eleme egy speciális árnyékolt kábel. Általában 300 méternél hosszabb kerítések vagy falak esetén javasolt az alkalmazásuk. Az érzékelő kábel hajlításai által keltett jeleket vizsgálva egy feldolgozó rendszer képes a behatolásra jellemző jelformákat azonosítani. Drótfonatos, rácsos kerítéseknel kiválóan alkalmas annak jelzésére, ha valaki átvágja a kerítést, átmászik rajta, vagy alul felemelve próbál bejutni. Speciális kompozit árnyékolt kábel használatával 3 méteres pontossággal meghatározható minden vágási, mászási kísérlet. Az érzékelő kábelek lehetnek elektret technológiájú koaxiális kábelek, piezo-elektromos koaxiális kábelek és lineáris mágneses érzékelő kábelek egyaránt.

⁸ Global System for Mobil communication, Groupe Spécial Mobile

2. Optikai szálak eszközei: az optikai szál, mint érzékelő sokkal kedvezőbb tulajdonságokkal rendelkezik, mint hagyományos fémvezetős megoldások, hiszen nem érzékeny az elektromágneses interferenciára, elektromos zavarokra, nagyfeszültségű kábelek jelenlétére. Működési elve arra épül, hogy a kerítés átvágása vagy átmászása esetén az optikai szál elhajlik, így a szálban vezetett fény intenzitása, illetve más tulajdonságai megváltoznak. A kábel kimenetére kötött vevőegység kiértékeli a lézerfény intenzitás-változásának mértékét, jellegét és az előírt küszöbszintnél nagyobb változás esetén riasztási jelzést ad. Az optikai szálakat drótfonatos, hegesztett fémhálós kerítéshez, téglafalhoz, épületfalhoz is lehet rögzíteni, illetve falban vezetni. Egyes optikai megoldások (pl. FOIDS⁹) akár 60 km-es érzékelési hosszúságot garantálnak, aktív eszközök (erősítők, ismétlők) közbeiktatása nélkül. Ez egy kiemelt fontosságú objektumoknál alkalmazott speciális megoldás, amikor az optikai szál egy különleges kiképzésű (GYODA¹⁰ szerű szögesdrót) éles acél szalagba van belepréselve (2. ábra), ahol ennek szakadása váltja ki a jelzést.



2. ábra: Az ún. NATO-drót szerkezete (forrás: <http://oktel.hu/>, letöltve: 2012. 04. 12.)

Az érzékelő kábeles kerítésvédelem magas kiépítési költségű és karbantartás-igényes védelmi rendszer, ezért jellemzően csak állandó őrszemélyzettel rendelkező kiemelt objektumoknál használják. Megbízhatósága miatt gyakran alkalmazzák a stratégiai fontos objektumok biztonsági rendszerének részeként, például katonai bázisok, börtönök, ipari-, vegyipari- vagy nukleáris létesítmények, erőművek védelmének.

⁹ Fiber Optic Intelligence & Detection System

¹⁰ gyorsan telepíthető drótaskadály

3. Falbontás érzékelők: szükségesek a gyengébb téglafalak, ritkán látogatott helyek védelméhez. A falbontás érzékelők típusai: fémháló és rácsvédő huzalozás, riasztótapéta és rezgés érzékelő. A legegyszerűbb és egyben legelavultabb megoldások egyike a fémháló és rácsvédő huzalozás alkalmazása.

A fémháló egyszerűen a vakolat alá helyezett vezető szál, amely hullámvonalban végigfut az egész falfelületen. Telepítése és – behatolás, vagy véletlen szálszakadás esetén – a javítása nehézkes és költséges.

A rácsvédő huzalok a nyílászárók rácsozatának elektronikus védelmét szolgálják. A rácsok felületére hátulra, vagy csőszerkezetes rács esetében akár a szerelvény belsejébe szigetelt vezeték (0,2-0,3 mm átmérőjű) kerül, ami sérülésre vagy vágásra jelzést vált ki. A szabotázs védelem miatt a vezető szálakat és a csatlakozási pontokat célszerű rejtetten kialakítani.

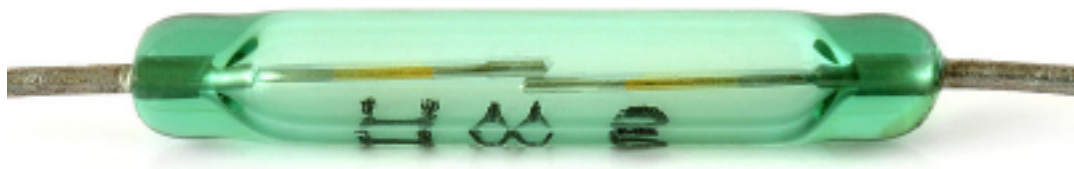
Riasztótapéta: különleges kétrétegű tapéta, amely a fémháló analógiája alapján működik. Az alsó réteg szigetelt vezeték, a felső réteg pedig takarásra, rejtésre szolgál. Falra, ajtóra stb. ragasztva védelmet biztosít, mivel átszakításakor a huzal sérül (folytonossághiány keletkezik), amire válaszul a riasztó jelzést ad.

A rezgésérzékelők között található mechanikus, indukciós és piezoelektromos elven működő típus is. Ez utóbbinak lényege, hogy bizonyos kristályokban mechanikai erő (deformáció) hatására elektromos feszültség jön létre. Az érzékelő házában egy kisebb fémtömeget helyeznek el, ami egy piezokristály lapkán keresztül csatlakozik a házhoz. Rezgések, ütések hatására a fémtömeg gyorsul és a gyorsításhoz szükséges mechanikai erő a gyorsulással arányos feszültséget kelt a piezokristály lapka felületein.

A „testhang,, érzékelők az ütő, vágó és feszítő eszközök alkalmazásai ellen nyújtanak hatékony védelmet, kiválóan alkalmasak például bontókalapács, fúró, gyémántfűrész, hidraulikus nyomó, hegesztő, vagy a lángvágó által keltett rezgések detektálására. Ezek az eszközök általában a 6-20 kHz közötti frekvenciasávba eső rezgéseket keltenek, így az érzékelők is erre a tartományra a legérzékenyebbek. A testhang érzékelőnek több típusa létezik: vannak egyszerűbb és intelligensebb verziók. Az egyszerűbb testhang érzékelők, mint például az ütésérzékelő csak egy-két falbontási módszer, jelen példában az ütvefúró és a bontókalapács ellen védenek. Az intelligensebb eszközök már az összes falbontási módszert képesek jelezni. Jellemző rájuk a digitális, mikroprocesszoros jelfeldolgozás. Működésük során felismerik és analizálják a különböző típusú rezgéseket és eltárolják

azokat. Amennyiben az adatok elemzése során valamelyik kritikus komponens szintje meghalad egy előre meghatározott küszöbértéket adott időintervallumban, az eszköz riasztást generál. Robbantás esetén azonnali, fűrés, lángvágás esetén 5-10 másodperc, kalapálás esetén pedig 1-2 perc a riasztáshoz szükséges idő. Hatósugaruk erősen függ a védendő fal anyagától (pl. acél esetén jóval nagyobb, mint betonnál), és a „támadó” eszköz típusától (1,5 - 15 méter). A telepítés, a detektorok érzékenységeinek beállítása során figyelembe kell venni, hogy számos zavarforrás lehet az érzékelők környezetében, amelyek téves riasztásokat eredményezhetnek. Zavart kelthetnek az épületgépészeti berendezések (liftek, szellőző rendszerek), a takarítógépek, a víz-, fűtés- és szennyvízcsövekben áramló folyadékok rezgései is.

4. Nyitásérzékelők: a nyílászárók megfigyelésére alkalmazott eszközök, vagyis egy adott ajtó vagy ablak nyitott, illetve zárt állapotának érzékelésére szolgálnak kül-, vagy beltéri használat esetén egyaránt. Kezdetben mechanikus érintkezőket, majd mikrokapcsolókat alkalmaztak, melyeket mára szinte teljesen kiszorított a reed relé¹¹. Ennek előnye, hogy működésükhöz nincs szükség külön energiaellátásra. Hosszú élettartam, akár 5-6 cm kapcsolási távolság és stabilabb kontaktus (aranyozott érintkezők) jellemzi. Külső mágnessel a reed zárva tartható a nyílászáró nyitásakor is, ezért árnyékolással, vagy kiegyenlített (duál) reedel lehet védekezni a szabotázs ellen.



3. ábra: Reed relé (forrás: <http://ob121.com>, letöltve: 2012. 04. 12.)

A reed relé tokozása többnyire műanyag, de nagyobb mechanikai igénybevétel, vagy vasajtók esetén gyakran alkalmaznak réz, bronz, vagy alumínium burkolatú érzékelőket is. Garázskapuknál, ipari kapuknál a robusztus kivitelű, nagy mechanikai szilárdságú fémtokos nyitásérzékelőket alkalmazzák, amelyre akár gépkocsival is rá lehet hajtani.

5. Az üvegtörés érzékelők a nyitásérzékelőn kívül a héjvédelem leggyakrabban használt eszközei, melyek az üvegezett nyílászárók (ablakok) és határoló felületek (kirakatok,

¹¹ A reed relé kisméretű, védőgázzal töltött zárt üvegcső, amelyben két, egymáshoz közel lévő, de egymással nem érintkező ferromágneses elektróda található. Mágneses tér hatására zár a kontaktus.

vitrinek, üvegfalak) megfigyelésére alkalmasak. Az üvegtörés érzékelő feladata a különböző típusú az üvegek (sík-, rétegelt-, dróthálós-, edzett-, termo- vagy fóliázott) betörésének észlelése. Az alkalmazott technológia szerint megkülönböztethetünk ragasztott, optikai, akusztikus és fémszálas üvegtörés érzékelőket.

A ragasztott kivitelű érzékelő mechanikai kontaktusba kerül az ablaküveggel, mert magára a védendő üvegfelületre ragasztják fel, amelynek törésekor keletkező rezgéseket érzékeli. Ma már gyakorlatilag nem használják. Korábban kétféle típusát a higanykapcsoló és a piezo érzékelőt alkalmazták. Higanykapcsolós üvegtörés érzékelő esetében egy fémcsövében két érintkező és egy higanycsepp kerül elhelyezésre. Az ablaktörés esetén létrejövő elmozdulást a higanycseppet elmozdítja, ami rövidre zárja a két érintkezőt riasztást okozva ezzel. Környezetvédelmi szempontok miatt a higanyos megoldást ma már legfeljebb csak vitrinek védelmének alkalmaznak. Piezo érzékelő esetében egy piezoelektromos lapkát ragasztanak az üveg felületére. A piezo kristályok alakja rezgések hatására megváltozik mechanikai, és ezáltal villamos feszültséget is generálva, ami arányos lesz az üvegfelületen keletkező bármilyen rezgéssel. A ragasztott érzékelők hatótávolsága 2-3 méter, manapság már elavultnak számítanak, mert kevésbé esztétikusak, nehezen szerelhetők, és csak magát az ablaktörés tényét jelzik, valamint számos téves riasztást is előidézhetnek rezgésérzékenységük miatt. Emellett gazdaságtalanok is, hiszen minden egyes ablaktábla külön érzékelőt igényel, esetleges ablakcsere esetén pedig új üvegtörés érzékelők beépítésére van szükség.

Optikai üvegtörés érzékelőt kiemelt fontosságú épületek védelmének alkalmaznak. Maga az eszköz két részből, egy adóból és egy vevőből áll. Az adó polarizált infravörös sugarakat küld az üveg felületére. Ha valamilyen fizikai behatás, pl. üvegtörés során megváltozik a sugárzás beállított visszaverődési törésszöge vagy fázisa, a vevő ezt érzékeli, és riasztást vált ki.

Az akusztikus üvegtörés érzékelő a jelenleg leginkább preferált eszköz, mind szerelhetősége, mind pedig működési elve alapján. Ezt az érzékelőt nem az üvegtáblára, hanem az üvegfelület mellé, vagy azzal szemben kell felszerelni. Az akusztikus üvegtörés érzékelő elhelyezhető falon, mennyezeten, vagy ablaktokon, tehát kivitelezése sokkal esztétikusabban, a helyiség adottságaihoz igazítva megoldható. A hatótávolsága is lényegesen nagyobb, mint az előző típusoké, 4-9 méter. Előnye emellett, hogy egyetlen érzékelő felhasználásával egyszerre több ablaktábla védhető, így jelentősen egyszerűbbé

és költséghatékonyabbá teszi az objektum védelmét. Az ilyen érzékelők az üveg törésekor keletkező és a levegőben terjedő rezgéseket érzékelik. Ezek a rezgések nemcsak az ember által hallható frekvenciatartományban jönnek létre, hanem sokkal szélesebb spektrumban. Üvegtöréskor 20 Hz alatti infrahangok és akár 100 kHz fölötti ultrahangok is keletkeznek. Az infrahangok a törés előtt, az üveg hajlásakor keletkeznek; az ultrahangok pedig a törés akusztikus hangjával együtt. A jellegzetes üvegtörés hallható hangja körülbelül 6kHz-es, a töréshang a hajlás hangját nagyjából 200 ms késleltetéssel követi. Ahhoz, hogy az érzékelő az egész törési folyamatot figyelni tudja kétcsatornás érzékelőkre van szükség. Az 1990 előtt gyártott érzékelők még jellemzően egycsatornásak voltak, azaz csak a töréshangra voltak érzékenyek. Hátrányuk, hogy telepítéskor az érzékenység beállításához üvegtörés szimulátorra van szükség, és a helyiség átrendezésekor újra kell kalibrálni őket. Önálló alkalmazásuk nem célszerű.

A fémszálas érzékelő az üvegtörés jelzésének egy olyan eszköze, amit magába az üvegtáblába dolgoznak bele, végeit pedig kivezetik. Hazánkban ez a fajta megoldás nem igazán terjedt el, egyrészt magas ára miatt, másrészt mert ezeket az üvegtáblákat nem lehet vágni, csak méretre gyártatni.

6. A felületvédelmet szolgálja az úgynevezett vagyonvédelmi szúnyogháló is, ami csak annyiban tér el a hagyományos szúnyoghálótól, hogy elektromos vezetékekkel van átszőve. Vágás, szakítás, és feszítés esetén riasztást vált ki.

Ezen eszközcsoporthoz vezeték nélküli kommunikációs megoldásokkal történő rendszerbe integrálásával összefüggésben a területvédelmi érzékelőknél megfogalmazott megállapítások érvényesek azzal a megszorítással, hogy felületvédelmi eszközök esetén sok esetben bár megvalósítható, mégsem biztos, hogy a leginkább költséghatékony megoldás a rádiófrekvenciás kommunikációs modulokkal ellátott érzékelők használata.

Épített objektumok, helyiségek védelme esetében ugyanakkor a technológia költségeinek csökkenése már lehetővé tenné Bluetooth technológián alapuló kis-hatótávolságú integrált érzékelők használatát, ugyanakkor ezek kereskedelmi forgalomban történő megjelenése és széleskörű elterjedése a felmerülő járulékos költségek miatt, még a kínált nagyfokú rugalmasság ellenére sem várható.

1.2 Elektronikus biztonságtechnikai rendszerek [1]

Bár a fentiekben tárgyalt érzékelők integrált vezérlés esetén akár autonóm működésre is képesek, gyakorlatban mégis legtöbbször rendszerben történő alkalmazásuk terjedt el. Ebben a részben a különböző funkciójú elektronikus biztonságtechnikai rendszerek kerülnek bemutatásra.

1.2.1 Behatolásjelző rendszerek

A behatolásjelző rendszerek feladata az emberélet és anyagi értékek támadás, rablás, betörés és lopás elleni védelme, továbbá a védett területre történő behatolás érzékelése, naplózása és jelzése. A köznapiban szóhasználatban az ilyen rendszereket nevezzük riasztórendszereknek. Ezek érzékelőkből, központokból, jelzőeszközökből, kezelő szervekből épülnek fel. Az érzékelőket, kezelőket és jelzőeszközöket a központokkal helyi kommunikációs hálózatok, a központokat a távfelügyelettel távfelügyeleti kommunikációs hálózatok kötik össze. A rendszerelemek összeköttetése régebben kizárólag vezetékes úton, mára természetesen az igényeknek és a környezeti feltételeknek megfelelően, a nagyfokú rugalmasság és alacsony telepítési idő miatt vezetékek nélküli átvitellel történik.

A védendő épületen találjuk a kültéri védelem eszközeit, míg az épületek falazatának, padlózatának, födémjének és nyílászáróinak védelmére a felületvédelem, vagy héjvédelem szenzorjai szolgálnak. Az épületen belüli mozgásokat a térvédelem eszközei követik, míg az nagyértékű ingóságok védelmét a tárgyvédelem biztosítja. A védett területen tartózkodókat veszélyeztető behatolók, támadások jelzésére a személyvédelem eszközei szolgálnak.

A rendszer jelzésre szolgáló elemei (akusztikus, vizuális) elhelyezhetőek helyben, vagy – távfelügyeleti szolgáltatással egybekötve – távol a védendő területtől. A helyben telepített jelző berendezések fény, hang vagy kombinált eszközök lehetnek.

A központi egység (vezérlő) kontrollálja a rendszerelemeket működését, folyamatosan (meghatározott időközönként) figyeli állapotukat, ellenőrzi működőképességüket. A hozzá csatlakozó a kezelőegységgel vezérelhetjük, élesíthetjük, „hangolhatjuk” a rendszer működését.

A leggyakrabban alkalmazott érzékelők:

- mozgásérzékelők (PIR, mikrohullámú érzékelő, kombinált érzékelő, infra sorompó stb.),

- nyitás és üvegtörés érzékelők a nyílászárókon,
- rezgés, fúrás érzékelők a falakban,
- kerítésvédelmi eszközök,
- támadásjelzők.

A behatolásjelző rendszer kiegészíthető füst-, gáz-, nedvesség és hőmérséklet érzékelőkkel, valamint alrendszerként integrálható az épületautomatizálási rendszerbe is. Az optimális objektumvédelmet úgy érhetjük el, ha a behatolásjelző rendszereket beléptető- és kamerás megfigyelő eszközökkel kombináljuk.

1.2.2 Beléptető rendszerek

A beléptető rendszer elsődleges feladata a belépni szándékozók azonosítása, a belépési jogosultság megállapítása, a belépés tényének naplózása, valamint az áthaladás szabályozása. Egy beléptető rendszer alapvető funkcionális egységei az olvasóterminál (pl. mágneskártya, vagy biometrikus azonosító), központi vezérlőegység, kezelő/monitor egység.

A beléptető rendszer elsődleges feladata a személy azonosítása, ami történhet a tulajdonában lévő azonosító eszköz felhasználásával, vagy az illető biometrikus jellemzőinek vizsgálatával, továbbá a leggyakrabban alkalmazott eljárással, a felhasználó tudás alapú azonosításával (PIN¹²-kód használata), illetve ezek közül bármely elem tetszőleges kombinációja alapján (több faktoros azonosítás).

Az azonosító eszközzel szemben támasztott követelmények:

- hordozza az adott beléptető rendszer és az eszköz tulajdonosára jellemző azonosítókat,
- legyen személyhez köthető, hamisítás, másolás ellen védett,
- nagy felhasználószám esetén is biztosítva legyen az egyedi azonosítás,
- a környezeti behatásokat adatvesztés nélkül viselje el,
- legyen kis méretű, könnyen kezelhető, esztétikus kivitelű,
- legyen sorozatban előállítható, olcsó.

A leggyakrabban használt azonosító eszközök a különféle kivitelű bankkártya méretű adathordozó/azonosító kártyák. Készülhetnek papírból egyszeri, vagy rövid idejű használatra

¹² **P**ersonal **I**dentification **N**umber – személyi azonosító szám

(pl.: belépő egy rendezvényre), illetve tartósabb kivitelben, tömör műanyagból, vagy több anyagból rétegelt.

Az azonosításra használt adathordozót számos technikai lehetőségéből lehet kiválasztani. A számítástechnikai eszközök elterjedése előtt még mechanikus, majd elektromos lyukkártyákat használtak, később következtek az induktív elven működő kártyák, a széles körben elterjedt vonalkódos azonosítók, majd a ferromágneses „rudacskákat” tartalmazó Wiegand rendszerű kártyák, amelyek 26 bites kódot tároltak. Később elterjedt azonosító eszközzé vált a mágnes-csíkkal ellátott kártya, viszonylag nagy adattároló kapacitást, ezáltal sokoldalú alkalmazhatóságot biztosítva (bankkártyák¹³).

Napjainkban az érintés nélküli azonosítási eljárások (RFID¹⁴) terjedése gyorsuló tendenciát mutat. Ezeknél a megoldásoknál a rádiós olvasóterminál és a kártya az elektromágneses hullámok útján, egymás érintése nélkül kommunikál. A kártyában egy keretantenna és egy mikrovezérlő¹⁵ található. A kártyák a tápellátásuktól függően lehetnek aktív kártyák, amelyek saját tápforrással rendelkeznek és lehetnek passzív kártyák, amelyek az elektronikához szükséges energiát a lekérdező egység elektromágneses teréből nyerik. Az érintésmentes olvasási eljárások előnyei: szabotázsvedett, nincs eltömhető nyílás, az olvasóterminál a fal síkjába illeszthető, rejthető, könnyen kezelhető és gyors azonosítást biztosít. Léteznek memóriakártyás azonosítók is, melyek közül a felületi érintkezősek terjedtek el széles körben (rég: telefonkártyák, ma: bankkártyák). Ezek nagy memóriakapacitással rendelkeznek, olvasásuk kóddal védhető.

A személyazonosítást szolgáló eszközök többsége másolható, hamisítható, de a legjobb technológiával védett kártyák sem jelentenek biztonságot a lopással szemben. Vagyis nem szavatolható, hogy a belépőket tévedhetetlenül azonosítani tudjuk. Régóta ismert, hogy az emberre jellemző biológiai jegyek a legjobb azonosítók, de azok hatalmas információtartalma miatt tárolásuk és gyors feldolgozásuk csak a számítógépek számítási teljesítményének megnövekedésével vált megbízhatóvá. Minden biometrikus azonosító rendszer működésének alapja, hogy a belépő személy vizsgált jegyeit korábban felvett és eltárolt mintákkal hasonlítjuk össze. A biológiai jegyek tárolhatóak a beléptető rendszer adatbázisában, illetve

¹³ Egy átlagos bankkártya személyi azonosításra, banki adatok tárolására használható, és beléptető kártyaként (számos bankfiók előtere) is funkcionál.

¹⁴ **Radio Frequency IDentification** – rádiófrekvenciás azonosítás

¹⁵ A mikrovezérlő, mikrokontroller egy olyan integrált áramkör, amely a processzorhoz hasonlóan egymást követő utasítások végrehajtásra lett tervezve, ugyanakkor az integrált áramköri lapka magába foglalja a programmemóriát, az adatmemóriát és a periféria illesztőket is (RS232, RS485, CAN, LIN, A/D, D/A, PWM, USB, Ethernet).

beírhatóak egy hordozó eszközbe (pl. memóriakártyába). Az ilyen rendszerek gyakorlatilag 100%-os azonosítási pontosságuk mellett sajnos lassúak és igen nagy beruházást igényelnek, ezért általában ott használatosak, ahol nagyon fontos területekre kevés személyt kell beengedni. Az azonosítás történhet ujjnyomat¹⁶, kéz geometriai jellemzői, érhálózata, szem vizsgálata (retina, írisz), beszédhang jellemzői, kézírás, illetve arc hőkép alapján [3].

Biometrikus beléptető rendszer tervezésekor figyelemmel kell lenni olyan tényezőkre, amelyek alapvetően befolyásolják a rendszer használhatóságát. A Föld népességének kb. 1-2%-a nem rendelkezik azonosítható ujjnyomattal, pontosabban az ujjnyomatot digitalizáló algoritmus nem tudja beazonosítani a keresett alakzatok, sajátossági pontok¹⁷ alapján. Nem szerencsés olyan munkahely beléptetését ujjnyom azonosításra bízni, ahol a munkafolyamatokból adódóan sérülhetnek vagy szennyeződhetnek az ujj mikrobarázdái.

Beléptető rendszerek tervezéséhez számos online kalkulátor nyújt segítséget, amellyel összehasonlíthatunk hagyományos és biometrikus rendszereket különböző paraméterek alapján. A <http://handyman.hu/roi-kalkulator> linken például egy kártyás és egy kézgeometriás azonosítási technológia ROI¹⁸ kalkulátort találunk.

Hangazonosítás	500:1
Arcfelismerés	2 000:1
Ujjnyomat azonosítás	1 000 000:1
Íriszvizsgálat	10 000 000:1
Retinaazonosítás	10 000 000:1

4. ábra: Néhány biometrikus rendszer FAR¹⁹ mutatója (forrás: <http://oktel.hu>)

¹⁶ Fontos megjegyezni, hogy a szakleírások is gyakran, de a termékleírások szinte mindig keverik az ujjlenyomat és ujjnyomat kifejezéseket. **Ujjlenyomat**nak nevezzük az ujjról készült jó minőségű képet, amely egy ujjvégi ujjperc teljes, körömtől-körömig történő körbeforgatásával készül (ezt veszik le a gyanúsított ujjáról). **Ujjnyomat**nak nevezzük az ujj síkfelületén keletkező általában jó minőségű lenyomatát. Ez az a kép, amelyet az általánosan használt képbeviteli eszközök le tudnak venni az ujjról. Értelemszerűen az ujjnyomat az ujjlenyomatnak csak egy részét tartalmazza. **Ujjnyom**nak (látens ujjnyomnak) nevezzük azt az ujjnyomatot, amelyet az ember azokon a tárgyakon hagy, amelyeket megérint. Ezek általában rendkívül rossz minőségű képet adnak és csak kis részét tartalmazzák a teljes ujjlenyomtatnak [4].

¹⁷ Sajátossági pont (minucia) – szabályosan elhelyezkedő látható elágazások, szigetek, villák, pontszerű képződmények, megszakadások, jellegzetes kezdő és végpontok.

¹⁸ Return on Investment – várható megtérülés

¹⁹ False Acceptance Ratio – téves elfogadási hányad

1.2.3 Távfelügyeleti rendszerek

Az előerős védelem leghatékonyabb módszere a távfelügyeleti rendszerek alkalmazása. A távfelügyelet révén az ország különböző pontjain lévő riasztó-, tűzjelző- és különféle segélyhívó rendszerek riasztásait, állapotváltozásait egy folyamatosan működő felügyeleti központ fogadja a helyi riasztáshoz képest jóval hatékonyabb védelmet biztosítva. A 24 órás távfelügyeleti szolgáltatás keretében a felügyeleti állomás diszpécerei egy számítógépes szoftver segítségével éjjel-nappal fogadják az ügyfelek rendszereiről – telefonos, rádiós, GSM, vagy GPRS kapcsolati formában – érkező kódolt jelzéseket. Ezeket regisztrálják, feldolgozzák, és szükség esetén intézkednek a megbízóval kötött szerződésben foglaltak szerint. A távfelügyeleti rendszerek lehetnek vezetékes rendszerűek: pl. kapcsolt vonalas telefonhálózat, beszédsáv feletti jelátviteli rendszer, bérelt áramkörös pont-pont összeköttetések, de felhasználhatóak a kábel TV hálózatok és természetesen a vezetékes informatikai hálózatok is.

A vezetékek nélküli felügyeleti rendszerek térhódítása miatt fontos megemlíteni, hogy az ellenőrizhetőség és a szabotázs elleni védelem miatt nagy fontosságú objektumok védelme esetén mindig autonóm átviteli rendszerekre, hálózatokra van szükség. Gondoljunk csak bele, hogy ha egy iroda ház távfelügyeleti rendszere az internetet használja átviteli közegnek, és az internetszolgáltatónál valamely hiba kapcsán megszűnik a szolgáltatás, akkor a távfelügyelet lehetősége is drasztikusan korlátozódik, legrosszabb esetben teljesen megszűnik.

1.2.4 CCTV²⁰ rendszer

A környezet megfigyelésében az érzékszervek közül látásnak van a legfontosabb szerepe, hiszen az agyunkhoz jutó összes információ mennyiségének közel 80%-át szemünk szolgáltatja, így a biztonságtechnikában is az események közvetlen vizuális megfigyelése és rögzítése döntő jelentőségű. A CCTV elnevezés azt jelenti, hogy a zárt láncú televíziós rendszer szolgáltatásai csak a felhasználók szűk, a hálózat kiépítése által meghatározott csoportja számára hozzáférhető. A CCTV olyan megfigyelő rendszer, ahol az érzékelő maga a megfigyelést végző személy, aki mérlegel és intézkedik szükség esetén. A megfigyelés térben és időben eltávolodhat az események helyszínétől és időpontjától, továbbá lehetőség van az emberi szem képességeit felülmúló érzékelés megvalósítására, valamint több, egymástól távol eső helyszín egyidejű felügyeletére is.

²⁰ Closed Circuit TeleVision

A videó megfigyelő rendszerrel számos helyen találkozhatunk a mindennapok során. Bankokban, bevásárlóközpontokban, repülőtereken, közterületeken, irodaépületekben, de már a kisebb üzletekben, családi házakban is egyre gyakrabban alkalmazzák ezeket a rendszereket. Alkalmazható üzleti célokra, főképpen a lopáskárok csökkentésére, sőt gyakran már az alkalmazottak ellenőrzésére, ipari és gyártási folyamatoknál a berendezések ellenőrzésére, megfigyelésére, térfigyelő kamerarendszerként bűnmegelőzési, bűnüldözési feladatokra.

A technológiai fejlődés irama ezen a területen különösen látványos, az eszközök képességei, műszaki paraméterei folyamatosan javulnak. A biztonsági kamerák felbontóképessége és az éjszaka is használható típusok fényérzékenysége egyre nő, miközben számos új funkció is megjelenik. Egyre erőteljesebb az IP²¹ alapú kommunikációt alkalmazó eszközök jelenléte, melyek fokozatosan szorítják ki az analóg technikát.

Egyre szélesebb körben terjednek az intelligens funkciókkal rendelkező IP és analóg kamerák olyan műszaki lehetőségeket biztosítva, melyek nemrég csak a tudományos-fantasztikus filmekben voltak fellelhetőek. Egy IP kamera egy megfelelő, fejlett alkalmazással ötvözve számos olyan funkciót elláthat, amelyhez korábban több különböző érzékelő, megfigyelő eszköz telepítése volt szükséges. Egy IP kamerával képesek vagyunk nappali és éjszakai (infra megvilágítással) videó felvételek készítésére, időzített állóképek, mozgásra exponált képek készítésére, a megfigyelés szempontjából jelentéktelen terület kitakarására (természetesen szoftveresen megoldással).

A mai biztonsági kamerák képfeldolgozó egységei a CCD²² és a CMOS²³ érzékelők. Bár mindkettő működése fotoelektromos effektuson alapul, a képkivétel módjának és a gyártástechnológiának az eltérése miatt jelentősen különböznek egymástól. A rendszerek legfontosabb eleme a kamera, de a működéséhez szükség van megjelenítők, és képrögzítő berendezések használatára is. Mivel egy CCTV rendszer általában nem csak egy kamerából áll, így egyszerre egy időben több kamera képét kell figyelni és rögzíteni. Gazdasági és egyéb okokból nem célszerű, hogy minden biztonsági kamera képét külön monitoron nézzük, ezért jelfeldolgozó eszközök segítségével egyetlen monitoron oldják meg több kamerakép megjelenítését. Ezek az eszközök: képléptetők, képosztók, multiplexek, mátrixok. A megfigyelés rögzítésére szolgálnak a videójel-felvevők vagy videójel-rögzítők. Régen analóg,

²¹ Internet Protocol – az internet és internetalapú hálózatok egyik alapvető szabványa. Ezen protokoll segítségével kommunikálnak egymással az internetre kötött csomópontok (számítógépek, hálózati eszközök, webkamerák stb.).

²² Charge-Coupled Device – töltés-csatolt eszköz

²³ Complementary Metal-Oxide Semiconductor – komplementer fém-oxid félvezető

ma már inkább csak a digitális rögzítést preferálják a jobb képminőség, gyorsabb kereshetőség és jóval hosszabb élettartam miatt.

A videojelek vezeték nélküli továbbítása ebben az esetben lényegesen eltér a szenzoroknál tárgyaltaktól, hiszen egy mozgókép lényegesen több információt tartalmaz, mint egy egyszerű vezérlő üzenet. Hagyományos felbontású analóg videojel továbbításához közel 6 MHz-es sávszélességre van szükség, amely alapvetően behatárolja az alkalmazás lehetőségét. Több kamerás analóg vezeték nélküli rendszerek létezésének napjainkban nincs létjogosultsága. Ugyanakkor a digitális kamerák megjelenésével megnövekedett az igény az ilyen jellegű megoldások iránt, hiszen a kínált rugalmasság ebben az esetben is vonzó szempont. Bár számos rádiófrekvenciás megoldás létezhet az ilyen eszközök rendszerbe történő integrálására, mégis az IP alapú szélessávú vezeték nélküli informatikai megoldások gyors fejlődése és elterjedése jelentheti az igazi alternatívát. Ugyanakkor biztonsági alkalmazásokról lévén szó, nagy hangsúlyt kell fektetni a polgári vezeték nélküli hálózati megoldások biztonsági kérdéseire.

Mivel a másik két szóba jöhető kommunikációs alternatíva önmagában még nem lehet versenyképes a fenti megoldással, így sem a mobiltelefon, sem pedig a műholdas rendszerek ilyen irányú alkalmazásával nem lehet a közeljövőben számolni.

1.2.5 Integrált felügyeleti rendszerek

A biztonsági fenyegetettségek sokrétősége számos különböző védelmi mechanizmus egyidejű működését kívánja meg, miközben a hatékony védelem szükségessé teszi e mechanizmusok együttműködését és integrálását is.

Az integrált biztonsági megoldások kidolgozásának alapkonceptiója az, hogy az egyes részterületeket érintő problémákra adott megoldások a legtöbb esetben nem nyújtják azokat az előnyöket, amelyeket a nagyobb területekre összpontosító, komplex, megoldások kínálnak.

Az integrált felügyeleti rendszerek egységes alapelvek és hálózati megoldások mentén biztosítják a hatékony mindenoldalú biztonsági felügyeletet. Ilyen rendszereket azzal a céllal terveznek, hogy a különböző alrendszerek (riasztó, tűzjelző, beléptető, CCTV) képességeit komplexen felhasználva, rugalmasan a konkrét feladathoz illesztve csökkentsék a maradék kockázatot minimálisra, ezáltal biztosítva kiemelt fontosságú katonai és polgári objektumok lehető legmagasabb szintű védelmét.

Ilyen rendszerekben az elemek és alrendszerek közötti kommunikációs hálózat kialakítása is gondos tervezést, illetve a rendelkezésre álló akár vezetékes, akár vezeték nélküli platformok komplex, sok esetben redundáns alkalmazását igénylik.

2 Elektronikus biztonságtechnikai rendszerek rádiófrekvenciás kommunikációs platformjai

A biztonságtechnikában alkalmazott elektronikus eszközök, érzékelők többsége már beszerezhető vezeték nélküli, elsősorban rádiófrekvenciás kivitelben is. Alkalmazásuk során számos olyan szempontot szükséges figyelembe venni, amelyek befolyásolják a végpontokat a központtal összekapcsoló, adott frekvenciájú rádiócsatorna minőségét, tulajdonságait, ezáltal kijelölve az alkalmazhatóság hatótávolság, adatátviteli képesség, és megbízhatóság szerinti korlátait. Ezeket befolyásolni képesek még az alkalmazott rádiófrekvenciás jelfeldolgozási eljárások, mint például a technológiafüggő moduláció és spektrumszórás, míg a kódolások és a rendszerbe épített információvédelmi technikai megoldások az információbiztonság szempontrendszer alapján határolják be a vezeték nélküli kommunikációs lehetőségek alkalmazhatóságát.

A fejezet második felében a nagy távolságú vezérlő-távfelügyeleti központ viszonylatban, az elsősorban épületeken belüli kis távolságú szenzor-vezérlő viszonylatban, valamint épületek közti, közepes hatótávolságú szenzor-vezérlő viszonylatban alkalmazható vezeték nélküli technológiák, valamint azok biztonsági kérdései kerülnek bemutatásra.

Természetesen a vezeték nélküli eszközök igénybevétele esetén az autonómiával és természetesen a rádiófrekvenciás teljesítmény előállításával, illetve kisugárással összefüggésben is merülnek fel energetikai kérdések, de azok részletes tárgyalása meghaladja ezen dolgozat kereteit.

Az elektromágneses sugárzás egymásra merőlegesen haladó (tranzverzális) az időben változó amplitúdójú (oszilláló) elektromos és mágneses erővonalak összessége, mely a térben hullám formájában terjed fénysebességgel, ezáltal energiát és impulzust szállítva. Ide tartoznak a rádióhullámok, mikrohullámok, az infravörös sugárzás, a látható fény, az UV-sugárzás, a lézer és a különböző részecskesugárzások egyaránt. Ezen hullámtípusok között az alapvető különbség frekvenciájukban (időegységek alatti rezgések száma) és ennek következtében hullámhosszukban van. A kapcsolat a frekvencia (f), a hullámhossz (λ) és az állandó fénysebesség (c) között a alábbi összefüggéssel írható le:

$$\lambda = \frac{c}{f}$$

A vezeték nélküli, rádiós átvitel biztonságtechnikai, illetőleg bármilyen célú felhasználását erősen szabályozott jogi háttér biztosítja. A kereskedelemben forgalmazott biztonságtechnikai eszközök nagy része az ISM²⁴-sávot használja, amely adott frekvencia tartományok meghatározott feltételek melletti felhasználását biztosítja igénybevételi költségek nélkül.

Az ISM sávokban működő berendezések többnyire kis hatótávolságú eszközök, amelyeket a szakirodalom SRD²⁵-nek nevez. Ezek olyan rádióadó és -vevő berendezések, melyek egy vagy kétirányú (beszéd, zene, kép, adat, vezérlés, stb.) jelátvitelt valósítanak meg rádióhullámok segítségével, és amelyek kisugárzott teljesítménye úgy van meghatározva, hogy más rádióalkalmazások üzemét ne zavarják. Az SRD-k legfontosabb ismérve, hogy használatuk során nem okozhatnak jelentős káros zavarást más felhasználások üzemében, és általában nem rádióengedély kötelesek.

Frekvencia	Hullámhossz	Alkalmazás
26,9-27,2 MHz	11 m	Rádiós távvezérlők, (<10mW)
40,6-40,7 MHz	7,4 m	Rádiós távvezérlők, (<10mW)
433,05-434,79 MHz	69,3-68,9 cm	10 mW, adás < 10%, csatornaszélesség korlátozás nélküli 1 mW, 100% csatornaszélesség korlátozás nélküli 10 mW, 100%, 25 kHz csatornák
868-868,6 MHz	34-34,5 cm	25 mW, <1,0%, csatornaszélesség korlátozás nélküli
868,7-869,2 MHz	34,5 cm	25 mW, <0,1%, csatornaszélesség korlátozás nélküli
869,3-869,4 MHz	34,5 cm	10 mW, 100%, 25kHz csatornák
869,4-869,65 MHz	34,5-34,4 cm	500 mW, <10%, 25kHz csatornák
869,7-870 MHz	34,4 cm	5mW, 100%, csatornaszélesség korlátozás nélküli

5. ábra: A biztonságtechnikában alkalmazott néhány VHF²⁶, UHF²⁷ frekvenciatartomány

ISM tartományok ipari, tudományos és orvosi célú, hatósági engedély nélkül működtethető berendezéseinek méteres és deciméteres tartományba eső sávjait az 5. ábra táblázata mutatja. A biztonságtechnikában leggyakrabban használt 434 MHz-en és 868 MHz-en egyaránt 1,74 MHz szélességű sáv áll rendelkezésünkre. Magyarországon a Nemzeti Média- és Hírközlési

²⁴ Instrumentation, Scientific, and Medical band – műszeres, tudományos és orvosi sáv (szabad sáv)

²⁵ Short Range Devices

²⁶ Very High Frequency – ultrarövidhullám (10 m - 1 m)

²⁷ Ultra High Frequency – deciméteres hullám (1 m - 10 cm)

Hatóság (NMHH) foglalkozik a frekvenciasávok kijelölésével és a hatósági engedélyek kiadásával. Az egyedi engedélyezéshez nem kötött sávokat és azok felhasználási feltételeit az internetes oldalán publikálja a NMHH a Frekvenciasávok Nemzeti Felosztási Táblázatban (FNFT)²⁸. A hazai szabályozás korlátozás nélkül átveszi az EU vonatkozó szabványos ajánlásait²⁹. Az ISM sávok kijelölése mellett a szabványok megadják az engedély nélküli felhasználás feltételeit, amelyek a kisugárzott adóteljesítmény korlátozása mellett az átvitel sáv szélességére és az adásidő kitöltési tényezőjére vonatkozó korlátozásokat rögzítik. A feltételek betartása szükséges ahhoz, hogy az SRD eszközök se egymást se más sávon működő berendezéseket ne zavarjanak.

A kisméretű SRD rádióeszközök szabványokban rögzített működési feltételeinek biztosítása és az olcsóbb előállításra való erős törekvés komoly kihívást jelent a tervezők számára.

2.1 Hagyományos rádiófrekvenciás átvitel alapvető tulajdonságai

Általában a 30 kHz és a 300 GHz frekvencia közötti elektromágneses hullámokat nevezzük rádióhullámoknak. Az összes rádiófrekvenciás berendezésre elmondható, hogy a kisugárzott rádióhullám energiája már kis távolságon belül is jelentősen csökken. Az energiacsökkenés a kisugárzás pontjától mért távolság négyzetével fordított arányos. A következő összefüggés³⁰ alapján az adóteljesítmény (P_A), a hullámhossz (λ), és a vizsgált távolság (d) ismeretében számolható a vett teljesítmény (P_v):

$$P_v = P_A \left[\frac{\lambda}{4\pi d} \right]^2$$

A rádióhullámok terjedésük során csillapodnak, visszaverődhetnek, elhajolnak, többutas terjedés esetén a vételi helyen erősíthetik és kiolthatják egymást. Ezen tulajdonságok jellemzésére, illetve leírására szolgál az abszorpció, a reflexió, a polarizáció és az interferencia, amelyekkel beltéri biztonságtechnikai alkalmazások tervezésénél fokozottan ügyelni kell.

2.1.1 Abszorpció

Az elektromágneses hullámok a tárgyakon való áthaladáskor jelentősen csillapodhatnak, vagy akár teljesen el is nyelődhetnek. A csillapodás mértéke függ:

²⁸ <http://www.nmhh.hu/index.php?id=dokumentumtar&mid=943>

²⁹ <http://www.etsi.org/WebSite/homepage.aspx>

³⁰ Izotróp antennákat feltételezve és nem számolva a szabadtéri csillapítással.

- a hullámhossztól,
- az anyag vastagságától,
- a felülettől (tömör, rácsos, hálós),
- az anyagjellemzőktől (nedvességtartalom, fémes tulajdonságok).

Egyszerű kísérletként tegyünk egy 3G-s üzemmódot (900/1900/2100 MHz) is támogató online mobiltelefon készüléket egy áramtalanított mikrohullámú sütőbe. Azt tapasztaljuk, hogy a készülék elveszti a 3G kapcsolatot, és visszaáll GSM (850/900/1800/1900 MHz) üzemmódra. A sütő ajtajában lévő árnyékoló fémháló alapvetően a 2,45 GHz-en működő berendezés sugárzását igyekszik a készülékben tartani, de a 3G-s sávok felső tartományát is hatásosan szűri³¹.

2.1.2 Reflexió

A fémes tulajdonságú anyagok reflektorként hatnak a rádióhullámokra, így azok nem vagy csak nagy veszteséggel, csillapítással képesek rajtuk áthaladni. A reflexiót jelentősen befolyásolja a fém (ajtókeretek, fémajtók, csővezetékek, fémszerelvények), vagy fémes (fémfóliák a hőszigeteléseken, fémgőzzel bevont hőszigetelő üvegezések vagy fémszekrények) felület kapcsolata a föld potenciállal. Egy földelt fémfelület elnyeli a kisugárzott jelet, a földetlen pedig visszaveri azt.

2.1.3 Polarizáció [5]

A polarizáció a rádióhullámok villamos térerősség vektorainak orientációját jelenti. Az antenna polarizációját az adja meg, hogy milyen orientációjú elektromágneses hullámok vétele esetén mutatja a legnagyobb érzékenységet. A polarizáció lehet lineáris, vagy cirkuláris (kör, vagy ellipszis). Lineáris polarizáció gyakorlati alkalmazásai esetében megkülönböztethetünk függőleges és vízszintes polarizációt, de lehetőség van köztes polarizáció kialakítására is. Függőleges antenna függőlegesen polarizált, a vízszintes huzalantenna, vagy rúd antenna vízszintesen polarizált rádióhullámokra érzékeny. Az eltérő polarizáció (adás és vétel között) esetenként 30 dB³² csillapítást is okozhat.

A polarizáció a terjedési tulajdonságokat is befolyásolja, mert a függőlegesen polarizált antenna elsősorban felületi hullámokat, a vízszintesen polarizált antenna pedig térhullámokat gerjeszt (természetesen az alkalmazott frekvenciatartomány tulajdonságaira figyelemmel). A

³¹ A Faraday kalitka elve érvényesül a hullámhossz tizedével összemérhető rácsátmérők esetén.

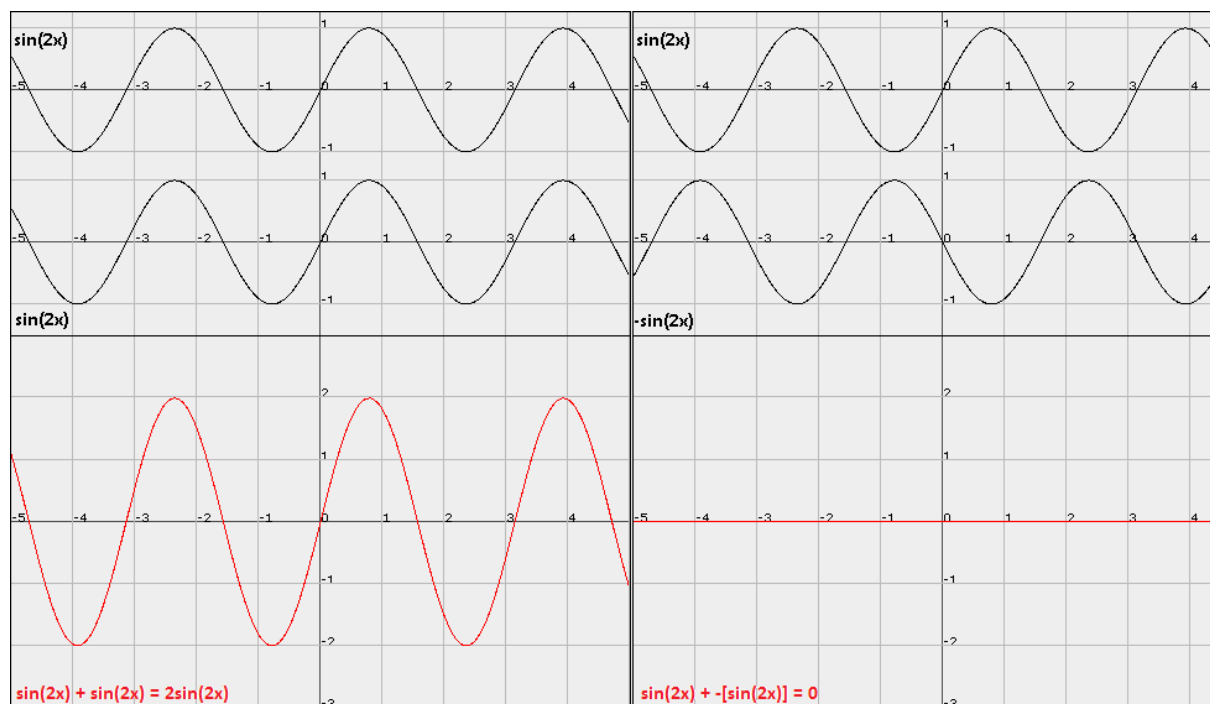
³² A 30dB-es csillapítás 1000-szeres teljesítményvesztést jelent.

legjobb vételi érzékenység akkor érhető el, ha az adó és a vevő antenna polarizációja megegyezik.

A rádióhullámok a (fém) felületeken nem csak tükröződhetnek, hanem akár a rezgési síkjuk is elfordulhat, azaz átpolarizálódhatnak. Ha az elfordulás 90° -os, a vevő antenna már nem képes venni a jelet.

2.1.4 Interferencia

Az interferencia egy olyan fizikai jelenség, ami akkor következik be, ha két különböző forrású, koherens³³ hullám találkozik, azaz olyan hullámok, amelyek fáziskülönbsége állandó. Interferencia során létrejönnek olyan pontok a térben, ahol a hullámok maximálisan erősítik, illetve olyanok, ahol maximálisan gyengítik egymást (annak függvényében, hogy az egyes pontokba a két hullám milyen fáziskülönbséggel érkezik).



6. ábra: Interferencia jelenség két szélsőséges esetben [6]

A 6. ábra bal oldalán látható az az eset, amikor két azonos frekvenciájú hullám azonos fázisban adódik össze, az eredmény a frekvencia változatlan, az amplitúdó kétszereződik. Az ábra jobb oldalán két azonos frekvenciájú, de ellentétes fázisú (180° -os eltolás) jel adódik össze, és eredményként teljes kioltás látható. A gyakorlatban azonban ritka ez a két szélsőséges eset, sokkal inkább az jellemző, hogy az interferált jel mind amplitúdóban, mind

³³ Két vagy több hullám akkor tekinthető koherensnek, ha forrásaik azonos fázisban rezegnek.

fázisban módosul az eredeti jelhez képest. A felületekről való visszatükröződés által – többutas terjedést okozva – is létrejöhet interferencia.

2.2 A GSM technológia biztonsága [7]

A mobiltelefon technológia széleskörű elterjedésével egyre nagyobb szerephez jut a biztonságtechnika területén is. Mára szinte alig kapható olyan biztonságtechnikai berendezés, amely ne tartalmazna GSM átjelzőt, vagy legalábbis ne lehetne bővíteni vele. A technológia segítségével széles körben elérhetővé vált, hogy távolról felügyeljük a vagyonvédelmi rendszereinket (behatoláskor, riasztáskor hívásértesítés, SMS), vagy akár beállítsuk a lakás fűtőrendszerének hőmérséklet-szabályozóját a megfelelő értékre.

Arra viszont már kevesebben gondolnak, hogy a mobiltelefon rendszerek által igénybe vett rádiócsatorna alapesetben semmivel sem védettebb más frekvencián üzemelő eszközökhöz képest, azaz a rádióhullám „befogásához” csak egy egyszerű vevőkészülékre van szükség.

A megfelelő biztonság kialakításához ezért a rendszernek biztosítani kell a végpontok azonosítását, a forgalmazás adatainak védelmét, sértetlenségét, valamint a beszéd- és adatforgalom biztonságát és integritását. Ehhez a rádióhullámokon továbbított adatokat titkosítani kell, hogy a küldött adatokat csak a valódi címzett tudja értelmezni. Az elektronika és a miniatűrízáció térhódításának köszönhetően azonban egyre gyorsabb és pontosabb rejtjelző eljárások, eszközök születtek, és egyre bonyolultabb matematikai algoritmusok használatára nyílt lehetőség. Egy-egy új technológia elterjedésének gátja a közös szabályozás hiánya volt, mígnem 1982-ben a francia székhelyű Postai és Távközlési Igazgatások Európai Értekezlete, a CEPT³⁴ létrehozott egy szabványt, amely az európai mobil telekommunikációs hálózat alapjává vált. A szabvány a GSM nevet kapta, és a megalkotása óta folyamatosan fejlődik (átalakul). A GSM technológia biztonsági rendszerének három alapköve:

- a felhasználók azonosítása;
- a rendszer működése során keletkező adatok titkosítása;
- a használók forgalmazásának (kommunikáció) titkosítása.

A felhasználók azonosítására a szabvány egy memóriakártyát ír elő. Ez az ún. SIM³⁵ kártya, a telefonkészülékben helyezkedik el, és tartalmaz minden, a kommunikációhoz szükséges

³⁴ Conference of **P**ostal and **T**elecommunications **A**dministrations

³⁵ **S**ubscriber **I**dentity **M**odule – előfizetői azonosító egység

adatot. Számunkra kettő igazán fontos ezek közül: az IMSI³⁶ azonosító és a Ki³⁷ kulcs. Az IMSI egy egyedi azonosító, amely a felhasználót azonosítja, rendszerint 15 számjegyből áll, ám bizonyos területeken lehet rövidebb. Az első három szám az ország kód³⁸, amit a szolgáltató azonosító kód követ. Amennyiben az eszközzel nem a honos³⁹ hálózatba jelentkezünk be, akkor az új szolgáltató az IMSI alapján egy TMSI⁴⁰-vel látja el az eszközt.

A Ki kulcs már sokkal izgalmasabb és titokzatosabb adat, ugyanis ez alapján végzi a kártyánk a titkosítást, illetve a titkosítás visszafejtését. A megfogalmazás itt most szó szerint értendő, ugyanis az adatokat nem a telefon titkosítja, fejtí vissza, hanem a SIM kártya, olyannyira, hogy a kártyából még a telefonkészülék sem tudja kinyerni ezt a számot. A Ki kód egy 128 bites egyedileg generált szám, amelynek a párja a szolgáltató adatbázisában található. Ez teszi lehetővé minden kártya számára az egyedi titkosítást. Ugyan nem tartozik a GSM szabványhoz vagy a szorosan vett hálózati biztonsághoz, de a SIM tartalmazza a jól ismert PIN és PUK⁴¹ kódokat, amiknek a felhasználók azonosítása során jutnak szerephez.

Az azonosításban tehát a Ki számnak van nagy szerepe. Egész pontosan úgy működik, hogy a hálózat küld egy 128 bites véletlenszámot a SIM kártyára, ami a kapott véletlenszám és a Ki számokból egy A3-nak nevezett algoritmus segítségével generál egy 32 bites azonosító számot (SRES⁴²). A SRES szám ezután elküldésre kerül a hálózatnak, amely összehasonlítja a saját SRES számával. Ez a challenge-response⁴³ elvű hitelesítés. Amennyiben nem egyezik a mobil állomás által küldött SRES a tárolt SRES-el, a hálózat megszünteti a csatlakozást a készülékhez. Ha egyezik, a telefon a véletlenszám és a Ki kulcsokból egy másik algoritmus, az A8 segítségével létrehoz egy titkosítási kulcsot, a Kc⁴⁴-t. Ezek után már minden készen áll a titkosított beszélgetéshez, és a készülékünk megkapja a központtól az engedélyt.

Az adatokat ezután megint egy új algoritmus, az A5 fogja titkosítani. Fontos megjegyezni, hogy amíg az A3/A8-at a szolgáltató választja meg, addig az A5 egy nemzetközi szabvány. Három változatát használják (bár jóval több is létezik) A5/1, A5/2 és A5/3 néven. Ezek közül az A5/2 az A5/1 gyengített változata, alacsonyabb biztonsági szinttel olyan országok számára

³⁶ **International Mobile Subscriber Identity** – nemzetközi mobil előfizető azonosító. Olyan egyedi azonosító szám, mely a SIM kártyán kerül tárolásra GSM és UMTS rendszerekben és a felhasználók azonosítására szolgál.

³⁷ **Individual Subscriber Authentication Key** – személyleíró hitelesítő kulcs

³⁸ Magyarország kódja: 216

³⁹ saját szolgáltatónk

⁴⁰ **Temporary Mobile Subscriber Identity** – ideiglenes mozgó előfizetői azonosító

⁴¹ **PIN Unblock Key** – PIN feloldó kód vagy: **Personal Unblocking Key** – személyes blokkolás feloldó kulcs

⁴² **Signed Response**

⁴³ kérdés-válasz

⁴⁴ **Cipher Key** – Titkosítási kulcs, 64 bit hosszúságú

készült, ahol a lehallgatás valószínűsége csekély. Az A5/3 (más néven Kasumi) egy 2002-ben, tehát jóval a GSM szabvány megjelenése után kifejlesztett algoritmus, amit az addig megszerzett tapasztalatok alapján dolgoztak ki, és egyelőre sokkal erősebbnek tűnik a másik két algoritmusnál. Ennek ellenére használata még nincs elterjedve. Magyarországon a három nagy szolgáltató az A5/1-et használja, amit már 1999-ben feltörték. Pár ezer eurós összegért megvásárolható olyan eszköz, amellyel a közvetlen közelünkben folytatott A5/1 vagy A5/2 titkosítási eljárással védett mobiltelefon beszélgetéseket lehallgathatjuk⁴⁵. A nagyobb védelmet nyújtó A5/3 szabványt jelenleg csak az UMTS⁴⁶ hálózatokban használják.

A titkosítás menete a következő: a Kc kulcsból és egy álvéletlen sorszámból (ami 0-tól megy kb. 2,7 millióig, ciklikusan) az A5 segítségével kapott szám aktuális bitjeit és a titkosítani kívánt adat bitjeit XOR műveletnek⁴⁷ vetik alá, és az így kapott bitek kerülnek továbbításra. A visszafejtés ugyanezen a módon történik. Természetesen, ha a számlálót szinkronizálni kell a két rendszerben, különben az eredmény értelmezhetetlen lesz.

A rendszer biztonságát növeli az a védelmi intézkedés, hogy – mivel az IMSI-t nem célszerű gyakran és kódolatlanul továbbítani – amint lehetséges, TMSI-t használunk helyette. A TMSI csak és kizárólag abban a cellában érvényes, ahol tartózkodunk, ezért minden váltásnál újat kapunk. Sőt, valahányszor a hálózatnak erre szüksége van, újat oszthat ki, függetlenül attól, hogy elhagytuk-e az adott területet, vagy sem. Az aktuális TMSI-t egy állandó memóriában tároljuk, ami a telefon kikapcsolása esetén sem törlődik.

2.3 Bluetooth [8]

A Bluetooth⁴⁸ vezeték nélküli szabványt 1998-ban kezdte el fejleszteni⁴⁹ öt világ cég (Nokia, Ericsson, IBM, Intel, Toshiba) azzal a céllal, hogy lehetővé tegye különböző készülékek közötti kábel nélküli összekapcsolást, ún. pikohálózatok létrehozását az éteren keresztül. A pikohálózat egy mester⁵⁰ és maximum hét szolga⁵¹ eszközből állhat. A szolga mindig csak a

⁴⁵ <http://statist.h16.ru>,
<http://gsm2interceptor.wordpress.com/2012/02/24/gsm-interceptor-price-list>,
<http://www.discoverytelecom.eu/catalog/2087.html>,
<http://www.tradevv.com/vs-2g-3g-4g-cdma-interception-gsm-interceptor>

⁴⁶ Universal Mobile Telecommunications System – általános mobil telekommunikációs rendszer

⁴⁷ másképpen megfogalmazva: (mod 2) összeadják

⁴⁸ Az elnevezés eredetileg egy a X. század második felében élt dán Viking királytól származik, akinek a neve Kékfog volt.

⁴⁹ A technológia megalkotója az Ericsson, eredetileg az RS-232 adatkábel vezeték nélküli változataként hozta létre a megoldást 1994-ben.

⁵⁰ master

mesterrel kommunikál és csak abban az esetben, ha a mester azt engedélyezi. A mester határozza meg az ún. Bluetooth csatornát és az órajel fázisát is, amelyet majd a pikohálózatban működő összes eszköz használni fog. A mester a csatorna meghatározásra a saját eszközcímét használja fel, amíg a szolga eszközöknek ugyanarra a csatornára egyforma fázisban kell hangolniuk.

A Bluetooth technológia egy széles spektrumú, full duplex, frekvenciaugráltatásos átvitelt használ, 1600 másodpercenkénti ugrással (a korábban említett, a mester által generált órajel a szinkronizált ugrási idők és a frekvencia szekvencia miatt lényeges). A rendszer a 2,402 GHz és 2,480 GHz közötti tartományban 79 vivőfrekvenciát használ, 1 MHz-es csatornaosztással. Néhány országban (például Franciaországban) ezt a frekvenciasávot szűkítették, és 23 vivős rendszert használnak. Mindkét rendszerben mind a frekvenciasáv alján, mind pedig a tetején van egy ún. védősáv is. A Bluetooth rádiómodul GFSK⁵² modulációt használ, amely a bináris egyest pozitív frekvencia deviációval, a bináris nullát pedig negatív deviációval modulálja.

Maximális adatátviteli sebessége elérheti az 1 Mb/s-os sebességet is. Egyaránt képes támogatni egy aszinkron adatcsatornát és akár három egyszerre működő hangátviteli csatornát, vagy egy csatornát, melyen egyszerre folyik adat és hangkommunikáció. A szabványt használó eszközök három nagy csoportba oszthatók energiafelhasználásuk alapján:

1. csoport: 1 mW átviteli energia, 0.1 - 10 méterig terjedő hatótáv,
2. csoport: 1-2,5 mW átviteli energia, 10 méternél nagyobb hatótáv,
3. csoport: kb. 100 mW átviteli energia, kb. 100 méteres hatótáv.

Mindhárom csoportba tartozó eszközök felhasználhatóak lehetnek különböző távolságokban felszerelt érzékelők központhoz történő csatlakoztatására.

2.3.1 A Bluetooth biztonságra

Minden Bluetooth eszköz három alapvető tulajdonsággal rendelkezik, miknek segítségével már a kapcsolódás kezdetekor biztonságra törekszik:

1. a Bluetooth eszköz címe, egy 48 bites cím, mely minden eszközben különböző,
2. a saját azonosítókulcs, egy 128 bites sorozat, amit az azonosítási procedúrák során használ a készülék,
3. a saját kódoló kulcs, egy 8-128 bit hosszúságú kódolásra használt kulcs.

⁵¹ slave

⁵² Gaussian Frequency Shift Keying – Gauss frekvenciaeltolásos billentyűzés

2.3.1.1 Kulcskezelés

A Bluetooth eszközök a biztonságos működéshez alapvetően összekötő⁵³ és titkosító⁵⁴ kulcsokat használnak. Az adatátvitel biztonságát az összekötő kulcs biztosítja, az átvitelre kerülő csomagokat pedig a titkosító kulcs védi.

Az összekötő kulcs egy 128 bites sorozat, ami az autentikáció ideje alatt használatos, valamint szerepe van a titkosító kulcs generálásában. A link key élettartama attól függ, hogy ideiglenes kulcsként hoztuk létre – amely az aktuális feladat elvégzése után megsemmisül –, vagy többször felhasználható kulcsként definiáltuk, amit akkor használunk, ha ugyanazt a feladatot többször is el szeretnénk végezni. Az összekötő kulcsok típusai:

*A kombinációs kulcs*⁵⁵: Az eszközök döntenek használatáról az inicializációs folyamat során. Amennyiben a használata mellett döntenek, a kulcs egyszerre jön létre a két kapcsolódó eszközben az E21 kulcsgeneráló algoritmus segítségével. Először generálnak egy véletlenszámot, a számot kombinálják a saját eszközcímükkel, majd kicserélik egymással véletlenszámaikat és kiszámítják a közösen használandó ún. kombinációs kulcsot.

*Az egység kulcs*⁵⁶: A Bluetooth eszköz első használatakor jön létre az E21 kulcsgeneráló algoritmussal. Létrejötté után eltárolódik a készülék memóriájában és itt gyakran cserélődik. Két eszköz a kommunikáció kezdeti szakaszában dönthet úgy, hogy egyikőjük egység kulcsát használják összekötő kulcsként. Ekkor általában a kisebb kapacitású eszköz kulcsmérete lesz a mérvadó, mivel előfordulhat, hogy az alacsonyabb teljesítmény, memóriakorlátok miatt nem tud nagyobb kulcsokat kezelni.

*Az elsődleges kulcs*⁵⁷: A kommunikációt vezérlő elsődleges eszköz által létrehozott ideiglenes kulcs. A generálásában két 128 bit hosszúságú véletlenszám és az E22 algoritmus vesznek részt. A 128 bit biztosítja számunkra, hogy ténylegesen véletlenszámot kapunk. Mind az elsődleges, mind az alárendelt, szolga eszközök egy "borítékot" generálnak az aktuális összekötő kulcs és a kulcsgeneráló algoritmus segítségével. A master eszköz bitenként össze XOR⁵⁸-olja a "borítékot" az általa létrehozott elsődleges kulccsal majd elküldi minden slave eszköznek, akik a "boríték" ismeretében megfejtik és alkalmazzák az új összekötő kulcsot.

⁵³ link key

⁵⁴ encrypting key

⁵⁵ combination key

⁵⁶ unit key

⁵⁷ master key

⁵⁸ kizáró-vagy, antivalencia

*Az inicializáló kulcs*⁵⁹: Akkor használják, amikor megkülönböztetés nélkül (nincs master és slave) kívánnak az eszközök kommunikálni egymással. Az inicializációs folyamat során mindkét eszközbe beviszik a PIN⁶⁰ kódot. Maga a kulcs az E22 alkalmazásával, a PIN kód, a kezdeményező fél eszközcíme és egy 128 bites véletlenszám részvételével jön létre. A kulcs használat után megsemmisül.

2.3.1.2 Titkosítás

A Bluetooth titkosítórendszere az átvitelre kerülő csomagok tartalmát titkosítja az E0 titkosító algoritmus segítségével, mely minden csomagot új folyamattal kódol. Ha egység kulcsot vagy kombinációs kulcsot használunk, az adatátvitel nem lesz titkosítva, de ettől függetlenül a belső adatforgalom lehet titkosított. Ha elsődleges kulcsot használunk, három eset lehetséges:

1. abszolút nincsen titkosítás,
2. az adatátvitel nem titkosított, de a belső adatforgalom az elsődleges kulccsal kódolt,
3. mindenféle adatforgalom titkosított az elsődleges kulccsal.

Mivel a titkosító kulcsok mérete 8-128 bites intervallumban változik, szükségessé vált, hogy az eszközök közös megegyezéssel kiválasszák a kommunikációhoz használt kulcsot. A "tárgyalás" kezdetén a master eszköz küld egy javaslatot a slave eszközöknek, melyek ezt elfogadhatják, illetve javasolhatnak egy másikat. Ez addig folytatódik, míg valamelyik javaslat elfogadásra nem kerül. Legtöbbször a kisebb kapacitású eszközhöz igazodik a titkosító kulcs mérete, mivel ezek adatfeldolgozó képessége erősen behatárolt, így előfordulhat, hogy egy túl hosszú kulcsot nem tudnának lekezelni. A legtöbb alkalmazás megszab egy minimális kulcsméretet, melynek megléte nélkül nem használható. Ez kiszűri azon eszközöket, melyek nem képesek kellő biztonsággal kommunikálni, így is csökkentve a támadhatóság mértékét.

2.3.1.3 Azonosítás

A Bluetooth eszközök az azonosítást kérdés-felelet formájában végzik el. A folyamat során használt protokoll szimmetrikus kulcsokat használ, tehát a sikeres azonosítás azon múlik, hogy minden kommunikációban résztvevő eszköz ugyanazt a kulcsot tette publikussá a többi számára. A kapcsolódási kérelem megérkezése után először az azonosító fél küld egy véletlenszámot a kérelmezőnek az azonosítás megkezdéseképp. Ezután mindkét eszköz

⁵⁹ initialization key

⁶⁰ Personal Identification Number – személyi azonosító szám, a Bluetooth szabványban hossza 1-16 számjegy között mozog. A hagyományos 4 jegyű PIN néhány alkalmazás számára nem elég biztonságos.

alkalmazza a véletlenszám, az aktuális összekötő kulcs és a kérelmező eszközcímének hármására az E1 függvényt, ami kiad egy értéket, az ún. digitálisan aláírt választ (SRES). Ekkor a kérelmező elküldi a választ az azonosító félnek, aki megvizsgálja, hogy a megkapott SRES megegyezik-e az általa kiszámított értékkel. Ha igen, a kérelmező sikeresen azonosította magát. Amennyiben az azonosítás sikertelen volt, egy bizonyos időnek el kell telnie az új folyamat megkezdése előtt. Ez az idő minden egyes sikertelen kísérlet után megduplázódik, mígnem eléri a maximálisan megszabott várakozási időt (ezzel megakadályozva a nyers erő alapú jelszótörést, az un.: brute force-t).

Legtöbbször a használt alkalmazás dönti el, hogy kinek kell azonosítania magát. Ez jelentheti a kérelmezőt, de előfordulhat, hogy a kiszolgálónak kell azonosítania magát. Ezeken az egyirányú azonosításokon kívül előfordulhat, hogy mindkét eszköztől megkövetelik az azonosítást. Ez a kétirányú autentikáció.

2.3.2 Bluetooth biztonságának gyenge pontjai

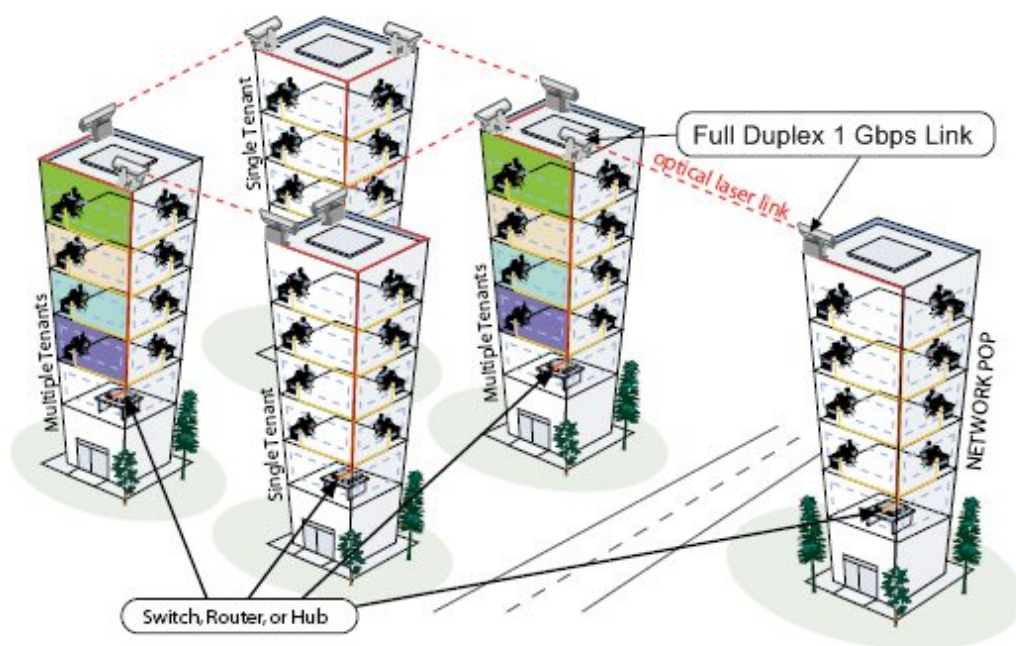
1. A titkosítási eljárásánál alkalmazott E0 algoritmus egy bonyolult matematikai eljárással feltörhető, és ezzel lehetővé tesz egy "oszd meg és uralkodj" típusú támadást. Ez akkor lehetséges, ha a megadott kulcssorozat hosszabb, mint az E0-ban használt legrövidebb kulcssorozat tároló/feldolgozó regiszter (LFSR⁶¹). Ez a támadási forma gyakorlatilag csak nagyon nehezen (vagy egyáltalán nem) kivitelezhető, mivel ehhez hozzá kellene férni a magas frekvencián (2.45GHz) működő eszközben még magasabb frekvencián üzemelő kódgeneráló algoritmushoz, amikor az frissíti tartalmát. Ez az idő azonban olyan rövid, hogy szinte lehetetlen megszerezni.
2. A csatlakozás kezdetekor minden résztvevő eszközbe külön-külön kell bevinni a PIN kódot. Ez egy nagyobb kiterjedésű ideiglenes hálózatban elég fárasztó lehet.
3. Az inicializációs kulcs egy sebezhető pontja lehet a rendszernek, mivel az egyetlen titkos résztvevője a kulcs generálásának a PIN kód. Ha ez a PIN kód négyjegyű, egy brute force eljárással aránylag rövid idő alatt kikövetkeztethetjük a PIN kódot, és az E22 algoritmus ismeretében kiszámolhatjuk az inicializációs kulcsot. Ehhez még hozzájárul az humán-tényező is, miszerint a PIN kódok többsége a „1234” és a „0000” sorozat (pl.: headsetek esetén), vagy a felhasználó születési éve.

⁶¹ Linear Feedback Shift Register

4. Támadásra alkalmas hiányosság fedezhető fel az egység kulcs kapcsán is. Tegyük fel, hogy „A” és „B” kommunikációjában „A” egység kulcsa az összekötő kulcs. Most tegyük fel, hogy „C” is csatlakozik a kommunikációhoz és ő is „A” egység kulcsát használja összekötőként. Ekkor „B”, mivel már korábban összekötő kulcsként hozzáfért „A” egység kulcsához, egy hamis eszközcím megadásával kiszámíthatja a titkosító kulcsot és lehallgathatja az „A” és „C” közötti adatforgalmat).
5. A teljesen egyedi eszközcímek lehetőséget adnak az eszköztulajdonos szokásainak megfigyelésére és annak dokumentálására, ami sérti az illető személyiségi jogait.

2.4 Lézeres adatátvitel

A lézeres adatátvitel – másnéven szabadtéri lézer (FSO)⁶² modulált látható vagy infravörös fénysugarak átvitelét jelenti a levegőn keresztül. Az adatátvitelhez a száloptikai kábelekhez hasonlóan fényt alkalmaz, az adatokat azonban nem az üvegszálás vezetéken át, hanem a levegőn keresztül továbbítja 7. ábra.



7. ábra: Átvitel szabadtéri lézerrel (forrás: <http://www.digitalairwireless.com>, letöltve: 2012.04.17.)

A szabadtéri optikai átviteli rendszerek természetesen akár 5-7 kilométeres távolságban is működhetnek, az elméleti maximális adatátviteli sebessége eléri a 160 GB/s-ot. A

⁶² Free Space Optics

kereskedelemben 100 MB/s és 2,5 GB/s sebességet támogató eszközök kaphatóak, amelyek szélessávú rádiófrekvenciás, mikrohullámú rendszereknek sáv szélesség korlátait messze túlhaladják, alapvetően pont-pont kapcsolat kialakításra képesek (pont-multipont esetében 1-2 km-es hatótávolsággal kell számolni).

A lézeres adatátvitel előnyei:

- A lézeres adatátvitel THz-es frekvencia sávban működik (600 GHz fölötti frekvencia spektrum még nincs szabályozva), ezért nincs túltelítve az alkalmazott tartomány.
- A telepítése, kiépítése gyors, és egyszerű (csak optikai rálátás szükséges).
- Lényegesen olcsóbb mint optikai kábeles kapcsolat.
- A lézeres hálózati architektúrán nem szükséges változtatni, amikor újabb csomópontokat adnak hozzá.
- Igen nehéz lehallgatni, mivel a sugarak keskenyek és irányítottak, valamint egy egyedi vevőt igényelnek. Illetéktelen hozzáféréshez szükség lenne valakire, aki az ablakon kívül lebeg egy másik vevővel, ami közvetlen kapcsolatban áll az adóval, és rendelkezik azokkal az ismeretekkel, hogy hogyan tudja összegyűjteni a jeleket. Mindezekon túl hamar kiderül, ha valaki megpróbál beavatkozni, ugyanis megszakad a hálózati kapcsolat. Továbbá a felhasználó és a hub közötti kapcsolat általában titkosított.

A hátrányok:

- A csomópontoknak akadálytalan rálátással kell rendelkezniük, az interferenciával számolni kell (időjárás, madarak).
- A zord időjárás a legnagyobb fenyegetés. Bár az eső és a hó torzíthatja a jelet, a köd a legveszélyesebb az átvitelre. A köd nagyon kicsi nedvességszemekből áll, amelyek olyan hatással vannak a lézerre, mint a prizma a fénysugárra: szétszórja és megtöri a jeleket.
- Az épületek az uralkodó szélirány hatására általában mozognak és kilengenek. Ez kétségkívül komoly probléma, hiszen az összeköttetések erősen irányítottak (1°), így a lézer csomópontoknak automata követő rendszerrel kell rendelkezniük, hogy kiegyenlítsék ezeket az elmozdulásokat.

3 Vezeték nélküli IP hálózatok biztonsági kérdései

Tekintve, hogy a vezetékek nélküli CCTV rendszerek kommunikációs vonalainak biztosítására az előző fejezetben tárgyalt technológiák adatátviteli képességeik szempontjából alkalmatlanok, egy korszerű integrált elektronikus biztonsági rendszer kialakításának feltételeit a jelenleg hozzáférhető technológiák közül csak IP alapú vezetékek nélküli informatikai megoldások lehetnek képesek biztosítani. Mivel azonban ez a polgári technológia mára széleskörben elterjedt, az ilyen alapú rendszerek elleni támadások száma is emelkedő tendenciát mutat. Fontos tehát megvizsgálni, hogy biztonsági szempontból ezek a hálózati megoldások alkalmasak, vagy alkalmassá tehetők-e biztonságtechnikai rendszerekben történő használatra.

Egy évtizeddel ezelőtt még az volt a jellemző, hogy az informatikai és biztonságtechnikai rendszerek külön hálózaton működtek. Manapság a biztonságtechnikai rendszereket költséghatékonyság miatt gyakran migrálják át IP alapú hálózatra. Ezért a vezetékek nélküli IP alapú hálózatok biztonságának megismerésével beleláthatunk abba, hogy mire kell számítani, ha a biztonságtechnikai rendszerünket erre a technológiára építjük.

A vezetékek nélküli hálózatok a fizikai tulajdonságaiból adódóan más biztonsági jellemzőkkel bírnak, mint vezetékes társaik. A vezetékes átviteli utaknál az adatot, a vezérlő vagy egyéb jelet hordozó rádiófrekvenciás jel terjedése a vezetékekben, vagy annak felületén, de mindenképpen a fizikai hordozó (optika, réz) közvetlen közelében történik. Ezzel ellentétben a vezetékek nélküli átviteli útnál az alkalmazott antennák karakterisztikájától függően akár a tér minden irányába kisugárzódik az átvinni kívánt rádiófrekvenciás jel.

Ahhoz, hogy a vezetékes rendszerünkhöz illetéktelenül hozzáférhessenek mindenképpen a fizikai réteg, a fizikai hordozó közelébe kell jutni. További nehézség, hogy a hozzáféréshez általában közvetlen csatlakozás szükséges, bár réz vezetők esetében néha elég a kábel közelébe jutás, indukzív elven detektálni a kábel által kisugárzott elektromágneses jeleket.

A rendszerhez való hozzáférést illetően a vezetékes átviteli utaknál jellemzően több és bonyolultabb eszközökre van szükség, mint a vezetékek nélküli társaiknál, ahol csupán egy

WiFi⁶³ kártyára van szükség. Adott esetben 100 méterről kapcsolódhatunk egy idegen vezeték nélküli rendszerhez, mert a rendszer biztonsági beállítása ezt megengedi, vagy 10 perces böngészéssel minden olyan információhoz hozzájutunk, amivel sajnos „megengedhetjük magunknak”.

Alapvetően elmondható, hogy a rendszerhez való hozzáférés problémája mindkét esetben megvan, de ezek a problémák a vezeték nélküli hálózatoknál gyakoribbak. Megoldást jelenthet az adminisztratív és műszaki eljárások alkalmazása és megfelelő intézkedések bevezetése.

3.1 WLAN⁶⁴ hálózatok biztonságos kialakítása [9]

A következőkben ismertetésre kerülnek a WLAN hálózatok biztonságos kialakításához és üzemeltetéséhez szükséges védelmi intézkedések.

3.1.1 Illetéktelen hozzáférés

A vezeték nélküli IP-t használó rendszerek esetében az illetéktelen rendszerhozzáférések jelentik az egyik legnagyobb problémát. A vezeték nélküli hálózatok és eszközök komoly fenyegetettséget jelenthetnek a rendszerek számára, ugyanis szabad belépési pontokat adhatnak a támadók és a rosszindulatú felhasználók kezébe. Sok esetben elég lehet egy hozzáférési pont⁶⁵, valamint egy WLAN kártya egy notebookba, és a jogosulatlan hálózati hozzáférés máris megvalósítható.

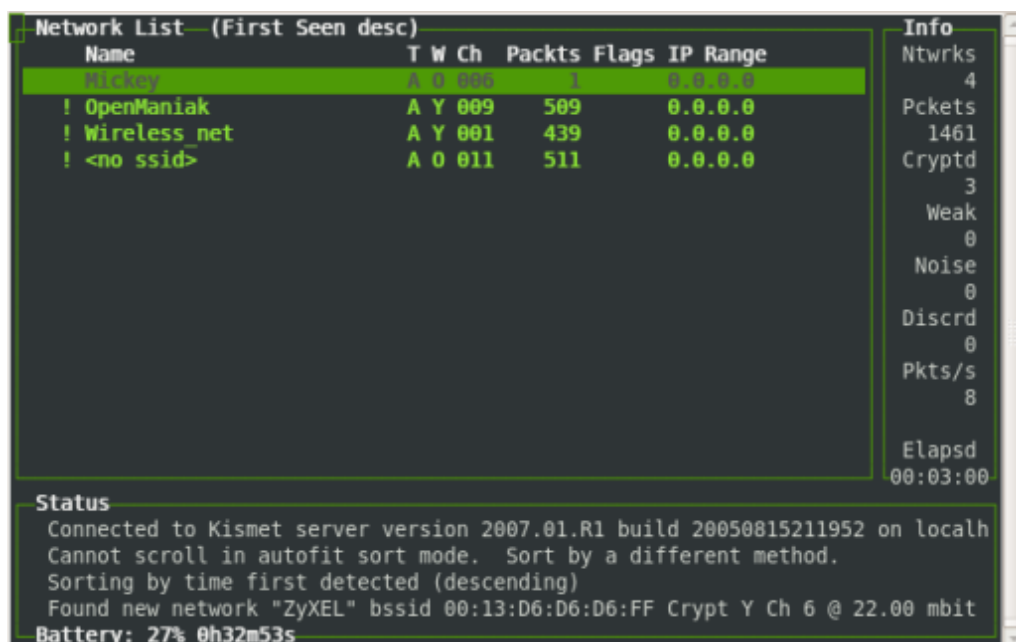
További problémát jelent, hogy általában a vezeték nélküli hálózatokhoz kapcsolódó eszközök alapértelmezésként olyan beállításokkal működnek, amelyek csekély biztonságot nyújtanak, és ezért könnyen felhasználhatók különböző támadásokhoz. Ugyancsak veszélyesek lehetnek az egymáshoz közel lévő vezeték nélküli hálózatok, ugyanis megvan annak a kockázata, hogy nem megfelelő konfigurációk esetén a két hálózat "összeakad" (pl. kézi frekvenciaválasztás esetén egymást interferálják).

⁶³ Az IEEE által kifejlesztett vezeték nélküli mikrohullámú kommunikációt megvalósító, széleskörűen elterjedt szabvány (IEEE 802.11x) népszerű megnevezése. (Egyes szakirodalmak a Wireless Fidelity rövidítésének veszik, mások csupán egy szójátéknak a HiFi után)

⁶⁴ wireless LAN – rádióhullámot használó vezeték nélküli helyi hálózat

⁶⁵ Egy cellát irányító bázisállomást neveznek hozzáférési pontnak (angolul: Access Point, AP)

A rendelkezésre álló megoldások közül több olyan is létezik, amelyek segítenek kiszűrni a jogosulatlan hozzáférési pontokat, és a hálózat sérülékenységét. Ezek közé tartozik például a NetStumbler⁶⁶ és a Kismet⁶⁷ (8. ábra) is.



8. ábra: Kismet alkalmazás (forrás: <http://openmaniak.com>, letöltve: 2012. 04. 01.)

Jó megoldás a sebezhetőségek kiszűrésére, ha egy sniffer⁶⁸ eszközzel végig járjuk a hálózat határait, és felderítjük az illetéktelen hálózati hozzáféréseket.

Sok biztonsági szakértő szerint a legjobb megoldást a folyamatos hálózatfigyelés jelenti. Ebből azonnal kiderül, hogy a felhasználók az adott hozzáférési ponton keresztül mikor csatlakoztak a hálózathoz, és mennyi adatot forgalmaztak. Ezek mellett az adatforgalom is valós időben monitorozható.

3.1.2 Hozzáférési pontok felügyelete

A vezeték nélküli hálózatok esetében is figyelmet kell fordítani a megfelelő határvédelem kivitelezésére. Fontos, hogy az aktív eszközök beállításainál a hozzáférési pontok SSID⁶⁹ azonosítóját lehetőleg módosítsuk a gyártó által alapértelmezettként megadottról, mert az eszközök dokumentációjából ezek az azonosítók bárki számára hozzáférhetőek.

⁶⁶ Aktív kapcsolatot próbál építeni minden, a környezetében található hálózati eszközzel.

⁶⁷ A vezeték nélküli hálózati kártyát monitor módba kapcsolva képes a hálózati forgalmat passzívan figyelni, sniffelni.

⁶⁸ A hálózaton továbbított adatcsomagok szemlélésére szolgáló hálózati segédprogram.

⁶⁹ Service Set Identifier

Tegyük egy gyors kísérletet az internet segítségével! Internetes kereső (google, yahoo! és bing próbálva) használatával a *router default password list* kifejezésre keresve rögtön az első találati oldalon megtaláljuk a <http://www.routerpasswords.com> oldalt, ahol gyártóra bontva kilistázhatjuk a vezeték nélküli eszközöket. A gyűjtemény modellekre bontva tartalmazza a hozzáférési protokollt, a gyárilag beállított felhasználói nevet és jelszót.

Természetesen, ha megváltoztatjuk az eszközökön a gyári hozzáférési beállításokat, azzal nem lesz hozzáférhetetlen a rendszer, de legalább nem „hirdeti” az eszköz a saját nevét és „hozzáférési kódját” a hálózaton.

Mivel a biztonságtechnikai rendszerek esetében igen jól behatárolható (még a tervezési fázisban), hogy milyen eszközök fognak csatlakozni a hálózathoz, ezért mindenképpen használni kell az elérési/csatlakozási pontokon kapcsolódó fizikai eszközök MAC⁷⁰ cím alapján történő szűrését.

Amióta a DHCP⁷¹ szerverek IP-címet és csatlakozást biztosítanak bárkinek, akinek fizikai kapcsolata van a hálózattal, a DHCP megkönnyítette a betöréseket. Védelem nélküli, vezeték nélküli hálózat esetén a DHCP bárkinek hozzáférést biztosít a sugárzás hatókörén belül a hálózathoz, beleértve az internet használatot és azokhoz az adatokhoz való hozzáférést is, amit mások nem védenek. Vezetékes hálózat (LAN) estén a támadónak fizikai kapcsolatra van szüksége, ahová a betörést nehezebb észrevétlenül kivitelezni. Ezért érdemes az IP-kiosztást manuálisan, MAC cím alapján megtenni.

A hozzáférési pontok rendelkeznek olyan biztonsági beállítással is, hogy képesek szűrni a kapcsolat adatforgalmának, átviteli sebességének figyelembe vételével. Ez a lehetőség akkor jön jól, ha távolról, és így limitált adatátviteli sebességgel próbálnak kapcsolódni a hálózathoz.

3.1.3 Titkosítás és autentikáció

A vezeték nélküli hálózatok biztonságának alapkövei a titkosítás és az autentikáció. Több módszer is elterjedt ezek megvalósítására, de az alkalmazásukkor nagyon körültekintőnek kell lenni. 2001-ben a kutatók és a hackerek is bemutattak olyan módszereket, amelyek a 802.11-es előírásoknak megfelelő WLAN hálózatokhoz tartozó WEP⁷² titkosítást hatástalanították. A

⁷⁰ **Media Access Control** – Egy hexadecimális számsorozat, amellyel a gyártás során látják el a hálózati eszközöket.

⁷¹ **Dynamic Host Configuration Protocol** – dinamikus állomáskonfiguráló protokoll

⁷² **Wired Equivalency Policy** – vezetékeskel egyenértékű (biztonságú) hálózat, mára korszerűtlen algoritmus a IEEE 802.11-ben meghatározott vezeték nélküli hálózatok titkosítására.

hackerek az Interneten olyan szoftvereket is közzétettek, amelyekkel szintén a WEP titkosítást lehet feltörni. A WEP könnyű feltörhetőségének bebizonyítása után sok fejlesztő cégnél megrendült a bizalom a WEP iránt, így a vezeték nélküli megoldások még védtelenebbé váltak.

A WiFi Alliance⁷³ által létrehozott WPA⁷⁴ tette lehetővé a biztonságos vezeték nélküli hálózati eszközök fejlesztésének megkezdését. A WPA az IEEE 802.1x-hitelesített kiszolgálókkal való együttműködésre lett kialakítva, amely különböző kulcsot rendel mindegyik felhasználóhoz. A hitelesítésben és titkosításban történt fejlesztéseknek köszönhetően a WPA-ban nagymértékben javult az adatcsomagok integritása. A WPA és WPA2 titkosítások esetében a felhasználók számára a kapcsolódáshoz biztonsági kulcs szükséges. Amikor megtörtént a kulcs ellenőrzése, a számítógép vagy egyéb eszköz és a hozzáférési pont között továbbított összes adat titkosítva lesz. Sajnos ma már azzal sem kell fáradozni, hogy feltörünk egy WPA, WPA2 jelszót, mert online szolgáltatásként 50 dollárért egy internetes cég megoldja helyettünk.

Mindezek ellenére a WLAN hálózatok esetében is lehet alkalmazni hatásos biztonsági megoldásokat. Ezek közé tartozik a RADIUS⁷⁵ szerverek használata, és a VPN⁷⁶ alkalmazása is. A VPN segítségével biztonságos kapcsolat építhető fel a végponti eszköz és a szerver vagy a tűzfal között. A RADIUS szerverek pedig az autentikációt támogatják annak érdekében, hogy a hálózati erőforrások elérése minél biztonságosabb legyen.

3.1.4 A vezeték nélküli hálózatok használatának szabályozása

Napjainkban a cégeknél már szükség van megfelelően összeállított biztonsági szabályzatokra. Ezeknek természetesen a vezeték nélküli hálózatok használati módjára is ki kell terjedniük. A szabályzatoknak tartalmaznia kell a WLAN eszközök biztonságára vonatkozó utasításokat, és a kezelésükkel valamint a karbantartásukkal kapcsolatos követelményeket. Az összeállításuknál azonban arra is ügyelni kell, hogy ne hozzunk olyan szükségtelen intézkedéseket, amelyek a hálózat hatékonyságát feleslegesen csökkentik.

A WLAN-hoz kapcsolódó szabályok közül a legfontosabbaknak a hozzáférési pontok használatával kell foglalkozniuk. Ezekben a szabályokban meg kell határozni, hogy ki veheti

⁷³ WiFi Szövetség

⁷⁴ Wi-Fi Protected Access

⁷⁵ A RADIUS egy autentikációs szerver.

⁷⁶ Virtual Private Network – virtuális magánhálózat. A VPN-en keresztülmenő adatok nem láthatóak az eredeti hálózaton, mivel titkosított adatcsomagokba vannak becsomagolva.

igénybe a hozzáférési pontokat, és ki, milyen beállításokat végezhet el azokon. Gondoskodni kell arról, hogy csak az arra kijelölt személyek módosíthassák a konfigurációkban szereplő WEP, SSID, VPN, stb. beállításokat. Szabályozni kell, hogy ki, milyen sebességű WLAN csatornához férhet hozzá, és milyen időpontokban használhatja azt. Természetesen ebben az esetben is igaz, hogy a leírt szabályok nem érnek semmit, ha azok betartatásával senki sem foglalkozik.

3.1.5 Behatolás érzékelés és megelőzés

A behatolás érzékelés és megelőzés nemcsak a vezetékes hálózatok esetében nagyon fontos. A WLAN hálózatokhoz is hatékonyan használhatók, és a segítségükkel a támadások még azelőtt kiszűrhetők még mielőtt azok elérnék a rendszer további, belső elemeit. Az IDS⁷⁷ megoldások a WLAN hálózatok esetében is 24 órás monitorozó funkciót látnak el, és használhatók a 802.11a/b/g protokollok esetében is. A folyamatos hálózatfigyelés révén nemcsak megakadályozhatók a támadások, hanem ki is elemezhetők. Protokoll analízisek, statisztikák és szabálymegsértési jelentések is készíthetők a segítségükkel.

Összefoglalva elmondható, hogy a vezeték nélküli hálózatok bevezetése és üzemeltetése kellő odafigyelés hiányában meglehetősen nagy kockázatot jelenthet a biztonságtechnikai rendszerekre. Azonban megfelelő, többszintű biztonsági intézkedésekkel hatékony és kockázatarányos védelem valósítható meg.

3.2 Támadási módszerek [10]

Manapság a vezeték nélküli rendszerek hálózatainak támadásához minden beszerezhető, legyen szó akár a fizikai eszközökről, akár a működtetésükre íródott szoftverekről.

A használatos alkalmazások nagy része, a csatlakozáshoz szükséges berendezések zöme akár kereskedelmi formában beszerezhető, illetve a szoftverek esetében az internetről szabadon hozzáférhető, letölthető.

Nagy hatótávolságú antennák használatával a csatlakozási távolság akár több 100 méterre növelhető, így viszonylag nagy távolságról képesek támadást folytatni a rendszer vezeték nélküli hálózatára. Ezek az antennák szintén megvásárolhatóak, vagy némi technikai készíttetéssel otthoni körülmények között megépíthetők (9. ábra).

⁷⁷ Intrusion Detection System – behatolás érzékelő rendszer



9. ábra: „WOK WiFi” (forrás: <http://tinypic.com>, letöltve: 2012. 04. 07.)

Egy átlagos wok⁷⁸ és egy hagyományos USB-s WiFi adapter párosítása látszik a 8. ábrán, ami jó esetben 15-18 dB-es jelnövekedéssel akár 2-3 km-es hatótávolságot eredményez. Parabolid felületet feltételezve kiszámolható a wok fókusztávolsága⁷⁹ és a legjobb erősítés érdekében oda kell helyezni a WiFi adaptert.

A vezeték nélküli kapcsolatok különböző hozzáférési kódokkal erősítik a hálózat biztonságát. A kódfejtéshez szükséges alkalmazások szinte egy időben a használt protokoll bemutatásával megjelennek, és hozzáférhetőek az interneten (WEPCrack, Aircrack: <http://www.aircrack-ng.org>). Az egyik leggyakoribb támadási forma War Driving⁸⁰, ahol a „nyitott” WLAN-okat térképezik fel (Netstumbler, Kismet), majd a GPS koordinátaikkal párosítva közzé teszi az interneten (<http://wigle.net>, <http://www.boingo.com>).

3.3 Támadási formák

3.3.1 Az aktív támadások általános formája

Széles körben alkalmazott eszközök segítségével a hackerek gyanútlan állomásokat tudnak létrehozni. Egy hacker első lépésként hozzáférési pontként (AP) funkcionál. Az „áldozat” gép requestet⁸¹ küld közvetve az AP-nak, majd az válaszüzenetet küld vissza, sőt ha szükséges, IP-címet is kap a rosszindulatú AP-tól. Innentől fogva pedig „szabad a vásár”: a támadónak teljes kontrollja van az áldozat hálózati forgalma felett.

⁷⁸ egy Kínából származó főzéshez használt edény

⁷⁹ $f_{parabola} = \frac{D^2}{16d}$ ahol „D” a parabola átmérője és „d” a parabola magassága

⁸⁰ Eredetileg a hálózatok nevének, helyzetének felderítésének örömről szólt, de gyorsan rosszindulatú tevékenységgé, mások által fizetett szolgáltatás hozzáféréssé alakult át.

⁸¹ kérést

Az ilyen támadások ellen a virtuális hálózatok (VPN) alkalmazása az egyedüli jó megoldás. A „biztonságos” hálózatok pedig monitorozzák az éter, s csak a hitelesített elérési pontokat engedik a hálózatukba kapcsolódni.

3.3.2 Visszaélés a MAC-címmel

Számos hálózat esetében a hitelesített MAC-címek listájával (ACL⁸²) teszi biztonságossá saját vezetékes nélküli hálózatát. Azonban a felhasználók könnyedén képesek MAC-címük megváltoztatására.

A különböző szoftvereszközök, mint például a Kismet vagy az Ethereal lehetővé teszik a hackerek számára, hogy megszerezzék egy hitelesített felhasználó MAC-címét, és ennek segítségével hitelesített felhasználóként tudnak csatlakozni a WLAN-hoz. A nagyvállalatok ezt a problémát is monitorozással küszöbölik ki, ugyanis kiszűrrik a szimultán használt MAC-címeket.

A WLAN betörő-detektáló rendszerek MAC-cím azonosításra is képesek a hálózati kártya gyártójának „ujjlenyomatát” analizálva, mivel a MAC-címek gyártónként előre kiosztottak.

3.3.3 Közbeékelés támadás (Man-in-the-Middle Attack⁸³)

Ennek során a kalózsok meg tudják törni a VPN-kapcsolat biztonságát a hitelesített állomás és az AP közé férkőzve. A rosszindulatú támadó az hozzáférési pont és az áldozat állomás közé állva képes magáról elhitetni a klienssel, hogy ő egy AP, az hozzáférési ponttal pedig, hogy ő egy hitelesített kliens. Kezdetben a hacker passzív, figyeli amint a kliens csatlakozik a hozzáférési ponthoz, s eközben a hitelesítéssel kapcsolatos információkat gyűjti csupán. Ezek felettébb fontos információk: felhasználónév, szervernév, kliens és szerver IP cím, a kliens által használt azonosító, valamint az AP által küldött hívó⁸⁴ és összerendelési⁸⁵ üzenet.

Mikor a hacker megpróbál az Access Pointhoz csatlakozni a megszerzett információk birtokában, az AP számára úgy tűnik, hogy egy hitelesített állomás kérése érkezik be hozzá. Az Access Point egy hívó üzenetet küld az általa hitelesítettnek vélt állomásnak, amely miután kiszámította a visszaküldendő választ, ezt válaszként vissza is küldi az Access Pointnak.

⁸² Access Control List – hozzáférés vezérlő listák. Egy mechanizmus, amely meghatározza az objektumhoz hozzáférhető felhasználókat ill. az objektumhoz való hozzáférés módjának típusát.

⁸³ A két fél közötti kommunikációt kompromittálja egy támadó úgy, hogy a kommunikációs csatornát eltérítve mindkét fél számára a másik félnek adja ki magát.

⁸⁴ challenge

⁸⁵ associate

A hacker állomás ezután szerzi meg az Access Point által kiküldött hitelesítési üzenetet, melynek segítségével már a kliens és az elérési pont közé állhat anélkül, hogy bármelyik is tudna erről, hiszen mindkét irányba tartó üzeneteket elkapja és továbbítja. A nagyobb hálózatokat üzemeltetők csak a 24x7 típusú monitorozásban látják ennek a támadási fajtának az egyetlen ellenszerét.

3.3.4 Lehallgatás

A vezetékek nélküli hálózat felhasználóinak saját érdeke, hogy a hálózaton átvitt érzékeny információikat megfelelő módon védjék lehallgatás ellen. Az esetek döntő többségében a felhasználók kezében vannak az ehhez szükséges eszközök. A megoldást rendszerint kriptográfiai eljárások használata jelenti.

A hálózat üzemeltetőjének nem feltétlenül feladata a felhasználók hálózati forgalmának lehallgatás elleni védelme. Természetesen amennyiben lehetősége van rá, akkor jó, ha az üzemeltető megszünteti vagy enyhíti a lehallgatás veszélyét.

A hálózat üzemeltetőjének feladata a felhasználók tájékoztatása a lehallgatás veszélyéről a lehetőségeknek megfelelően, hiszen ebben az esetben a felhasználók nagy része nem rendelkezik a szükséges ismeretekkel. Ezen túl elmondható az is, hogy a hálózat üzemeltetőjének több okból érdeke is a felhasználók tájékoztatása a lehallgatás veszélyéről csak úgy, mint a védelem a lehallgatás ellen. Egyrészt ugyanis az érzékeny információk lehallgatásából később adódhatnak más biztonsági incidensek a hálózaton, amivel az üzemeltetőnek is foglalkoznia kell. Másrészt a lehallgatás számtalan olyan esemény forrása lehet, amely a felhasználó megelégedettségét csökkenti, többek közt az üzemeltetővel is.

A lehallgatás ellen leginkább a felhasználók tudnak védekezni, a hálózat üzemeltetői csak hatalmas erőforrások árán tudnak ehhez hozzátenni. A felhasználóknak lehetősége van biztonságos, a hálózati forgalmat titkosító protollokat használniuk (pl. ssh, scp, SFTP, HTTPS, IPSec ESP), amelyek gyakorlatilag minimálisra csökkentik az érzékeny információk lehallgatásának veszélyét. Ezzel szemben az üzemeltetőnek nincs igazán jó lehetősége a lehallgatás elleni védelemre.

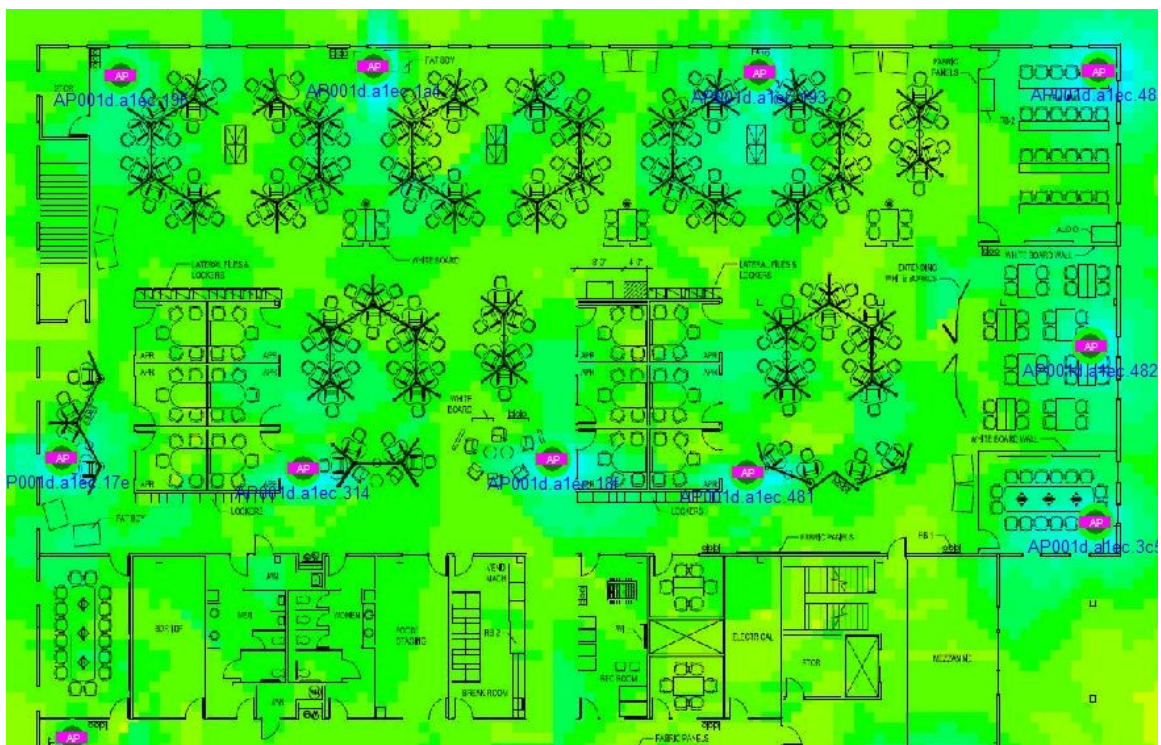
3.4 A vezetékek nélküli hálózatok biztonsága [11]

A vezetékek nélküli rendszerek számos oldalról veszélyeztetve vannak. A veszélyeztetés megvalósulhat szándékos és véletlen okokból kifolyólag. A rendszer biztonságát fenyegető

alapvető veszélyek nagy része a szándékos „támadások” esetébe tartozik. Ilyenek a jogosulatlan hozzáférés, a forgalommonitorozás, és a szolgáltatás megtagadása.

3.4.1 Forgalommonitorozás

A forgalommonitorozás jellemzően a nem titkosított hálózatok adatcsomagjait ellenőrzi. A hozzáféréshez elég a vezeték nélküli rendszer hatósugarán belül tartózkodni, és a jogosulatlan felhasználó mondhatni játszi könnyedséggel férhet hozzá a hálózaton továbbított adatokhoz (pl. egy beléptető rendszer esetében a rendszerbe felvett RFID kártyák azonosítójához).



10. ábra: A lefedettség megjelenítése az AirMagnet Surveyor Pro segítségével (forrás: <http://www.cisco.com>, letöltve: 2012.04.09.)

A vezeték nélküli hálózat felméréséhez, monitorozáshoz, akár a továbbított adatcsomagok kifejtéséhez nyújt segítséget pl. az AirMagnet alkalmazás csomag (10. ábra).

Megoldást jelenthet a monitorozás ellen a végpontok közötti titkosítás alkalmazása, azaz titkosítanunk kell a bázisállomás és a vezeték nélküli hálózati eszköz között. Ez a hasznos tartalmat (payload⁸⁶) alakítja át egy a titkosításra jellemző algoritmus, és a felhasználók által meghatározott kulcs szerint, így megnehezítve a jogosulatlanok számára az elcsípett adatok visszafejtését.

⁸⁶ hasznos

3.4.2 Jogosulatlan hozzáférés

Egy vezeték nélküli biztonságtechnikai rendszer, sőt bármely vezeték nélküli rendszer esetében figyelembe kell venni azt a lehetőséget, hogy a monitorozáshoz hasonlóan bárki hozzáférhet a rendszerhez. Pl. ha egy vezeték nélküli CCTV rendszer esetében a kamerák felvételeit egy központi szerveren naplózzuk, és a szerver és a végberendezések között valamely szabványos vezeték nélküli hálózatot használunk adatátvitelre, akkor nem megfelelő védelem esetén nagyon könnyű hozzáférni a szerver merevlemezei tárolt adatokhoz, vagy akár a CCTV rendszert vezérlő alkalmazáshoz is.

A helyzetet súlyosbítja, hogy a vezeték nélküli hálózatoknál az eszközök 20-30%-ban a gyári beállításokkal működnek, de hasonlóan rossz arány jellemzi a biztonságtechnikai berendezések beállításait is.

Az operációs rendszerek automatikus csatlakozási kísérleteik a már ismert SSID-jű hálózatok felé további veszélyeket rejt (lásd: Kovács Zsombor 2010 hacktivity előadása).

A informatikai veszélyek tekintetében a programozók által elkövetett hibák (hibás memóriefoglalás, felszabadítás, rossz változó, a bemeneti információ szűrésének hiánya, stb.) lehetőséget adnak a támadók számára, hogy a program futásában előidézett hibák, rossz kivételkezelések felhasználásával a saját kódját futassa le. A vezeték nélküli eszközök tekintetében a probléma ott kezdődik, hogy a hálózati kártyák meghajtó programjai (driver) rendszer szintű jogosultságokkal futnak, így azok kompromittálása az operációs rendszer feletti teljes kontroll átvételét jelenti (számos ilyen bug⁸⁷-ot fedeztek már fel). [12]

Az úgynevezett beágyazott rendszerek (embedded system) sérülékenységeivel is számos tanulmány foglalkozik, kiemelve korlátozott kapacitásuk (memória, CPU) következtében fellépő hiányosságokat (nincs tűzfal, hoszt iDS, antivirus).

Komoly veszélyt jelent az úgynevezett rogue access point, azaz csaló hozzáférési pont megjelenése a hálózaton. A rogue AP engedély nélküli hozzáférési pont, amelyet akár véletlenül is létrehozhat egy – a biztonsági előírásokat nem ismerő – felhasználó, vagy szándékosan a rendszerhez illetéktelenül hozzá férni kívánó személy. Az ilyen AP-k rendszerint védelem nélküli csatlakozással biztosítják, hogy bárki hozzáférjen a vezeték nélküli hálózathoz. Megoldást a hálózatüzemeltetők folyamatos hálózat monitorozása nyújthat.

⁸⁷ bogár

A hozzáférési pontok és a végberendezések közötti kölcsönös hitelesítés is megoldást jelenthet megelőzni az engedély nélküli hozzáférést.

3.4.2.1 Emberközpontú támadások

A hitelesítés és titkosítás növeli a vezeték nélküli hálózatok biztonságát, de nem akadályozza meg a hálózathoz való hozzáférést.

Az ember központú támadás gyenge pontja lehet a rendszereknek. Ennél a támadási formánál egy fiktív eszközt hoznak létre a felhasználó és a hálózat között. A leggyakrabban úgy veszik irányításuk alá a vezeték nélküli hálózatot, hogy az ARP⁸⁸ protokoll ellen indítanak támadást, mert ez a protokoll minden TCP/IP hálózatonál használatos.

A vezeték nélküli hálózat normál működése közben az ARP protokollal gyűjti be a célállomások hálózati eszközeinek fizikai címeit. A hálózati eszközöket összefogó szerver⁸⁹ ismeri a célállomások IP címét, de a fizikai címeket nem. A szerver üzenetszórással ARP kérést hirdet a hálózatban, amiben megadja a keresendő állomás IP címét. A hirdetés minden taghoz eljut, és az a tagállomás, aki felismeri a saját IP címét, visszaküldi a szervernek a saját MAC címét.

Nem túl bonyolult kijátszani az ARP protokollt. Az illetéktelen hozzáférőnek csupán annyi dolga van, hogy az eredeti címzett IP címével küld ARP választ a saját MAC címét megadva. A hálózaton az összes állomás frissíti az ARP tábláját a hamis MAC címmel, és ettől kezdve az állomások a hamis hozzáférési pontnak küldik az adatcsomagokat. A gyártók reagálva erre a biztonsági résre létrehozták a SARP⁹⁰ protokollt.

A SARP egy speciális biztonsági csatornát hoz létre a routerek⁹¹, hozzáférési pontok és a kliensek között, amely figyelemmel kíséri az olyan ARP válaszokat, melyek a csatorna ismeretlen helyéről érkeztek. Ezzel megakadályozzák, hogy illetéktelenek ne frissíthessék az ARP táblát. A megoldás hátránya, hogy minden tagállomáson firmware⁹² frissítést igényel. Másik megoldás, ha a statikus ARP bejegyzéseket teszünk minden alapértelmezett átjárót (default gateway) rögzítve.

⁸⁸ Address Resolution Protocol – címfeloldó protokoll

⁸⁹ A szerverek mellett az összes ethernet hálózati végpont az ARP protokollal rendeli össze a pont-pont összeköttetésekre használt címeket a végpont-végpont azonosításra szolgáló IP-kel.

⁹⁰ Secure ARP

⁹¹ útvonal választó eszköz

⁹² Az elektronikus eszközök vezérlését végző program

3.4.2.2 Szolgáltatásmegtagadás

A vezetékek nélküli hálózatok megbénításának egyik legnépszerűbb módja a DoS⁹³, azaz a szolgáltatásmegtagadás. Valós fenyegetettségről van szó, hiszen óriási következményekkel lehet számolni, ha egy hálózat – akár rövid időre is – működésképtelenné válik (lásd: Észtország 2007, Grúzia, Korea 2009). A következmények mértéke nagyban függ attól, hogy milyen feladatokra használjuk a vezetékek nélküli hálózatot.

A szolgáltatásmegtagadás egyik kiváltása a brute force módszerek alkalmazása. Ilyenkor annyi csomaggal (random adat, kérés stb.) árasztjuk el az állomásokat, hogy a sávszélesség lecsökken, hálózat erőforrásai elfogynak, és végül a hálózatot leállásra kényszeríti. Más megközelítésből a teljes kipróbálás módszerét nevezhetjük így, amikor a rejtjelező rendszer ismeretében az összes lehetséges kulcsot kipróbálva határozzuk meg az alkalmazott kulcsot.

A támadás akár egy helyről egy csomaggal is lehet eredményes (pl. ping of death⁹⁴), de az elterjedtebb megoldást a DDoS⁹⁵, azaz az elosztott szolgáltatás megtagadásos támadás jelenti. A DDoS esetében a támadó – egy eszköz helyett – átlagos számítógépekből kialakított hálózatot állít csatasorba, ahol a gépek felett átvett irányítással és az erőforrásuk összpontosításával sokkal nagyobb terhelést, nagyobb kárt tud okozni.

A szolgáltatásmegtagadás kiváltható elektronikai zavarással is, ahol a hasznos rádióhullámot egy erősebb – azonos frekvencia tartományú – jellel elnyomják, s így elérhetetlenné teszik a vezetékek nélküli hálózatot. Az efféle támadás viszonylag ritka, mert az elektronikai zavarást egy nagy teljesítményű adóval közélről kell végrehajtani.

A Tiger Team 101 epizódjában (a dokumentumfilm első részének linkje: <http://www.youtube.com/watch?v=cJIqqSj2xPs>) egy cég GSM elven működő riasztóját egy GSM zavaró segítségével semlegesítik. Ez a módszer bármely más átviteltechnikai rendszer esetén implementálható megfelelő szaktudással, így alternatív átviteli utak, egyéb intézkedések kialakítása szükséges a szabotázs elleni védelem érdekében.

Előfordulhat olyan eset is, amikor akaratlanul zavarjuk a saját rendszerünket. A vezetékek nélküli hálózat frekvenciatartományában működő egyéb eszközök párosulva egy egyébként is zsúfolt rádiófrekvenciás tartománnyal gyakran okoznak sávszélesség csökkenést, rosszabb

⁹³ Denial of Service

⁹⁴ A támadó nagyobb csomagot küld a szervernek, mint az kezelni tudna. Mivel egyes operációs rendszerek a tördelt csomagok esetén az utolsó csomag megérkezése előtt allokálnak memóriát, a csomag tartalmának összeállítása során ezt a memóriaterületet „túlírják”. Ez napjainkban már nem működő támadási forma.

⁹⁵ Distributed Denial of Service

esetben a rendszer teljes működésképtelenséget. Ezt a jelenséget hívjuk elektromágneses interferenciának (EMI⁹⁶).

A szolgáltatásmegtagadást eredményező támadások elleni védekezést jól megtervezett és alkalmazott biztonsági intézkedésekkel érhetjük el (bonyolult és sűrűn cserélt jelszavak alkalmazása, erős tűzfal, friss vírusvédelem, folyamatos programfrissítések használata, szenzorhálózat). A fizikai réteg támadása esetén megoldást jelenthet, ha a hálózati kapcsolatot automatikusan ellenőrzi a rendszer (pl.: a szolgáltató hálózati elemeinek rendszeres pingelésével, hiba esetén alternatív úton jelzés generálása).

A DoS támadások ellen nyújthat védelmet, ha megakadályozzuk, illetve korlátozzuk a vezeték nélküli hálózatunk jelének kedvezőtlen irányba való terjedését. Alapvetően ezt a cserélhető antennával rendelkező elemeknél a körsugárzókat irányított antennákra történő cserélésével oldhatjuk meg. Ha nem szeretnénk, hogy a rádiófrekvenciás jel kijusson egy épületből, akkor a hullámhosszt figyelembe véve szigetelő hálókat helyezhetünk a vakolatba, különböző fémfóliákat helyezhetünk az ablakokra, vagy fémszórt üvegre cserélhetjük le a hagyományos ablaküvegeket. Természetesen alapvető fontosságú, hogy a szigetelő felületek földeltek legyenek, hiszen nélküle antennaként sugározzák tovább a vezeték nélküli hálózat jelét. Ha magában és épületben is korlátozni szeretnénk a jelterjedést arra is vannak lehetőségek. Az aktív eszközök nagy részén beállítható a jelerősség, így limitálható olyan szintre, amire az adott hálózatnak szüksége van. Az úgynevezett wireless controllerek segítségével az AP-ok központilag konfigurálhatóak, azok jel zaj viszonya alapján frekvenciájuk változtathatóvá válik, idegen AP jelenlétében a kisugárzott teljesítmény növelhető.

Összegzésül elmondható, hogy a szolgáltatásmegtagadásra irányuló támadások ellen nem lehet tökéletesen védekezni, ami azt jelenti, hogy fel kell készülni arra az esetre, ha súlyos kár keletkezik a hálózatban. A biztonságtechnikai eszközök vonatkozásában elgondolkodtató, hogy a magas minőségigényű forgalom (folyam jellegű audió, videó tartalom pl.: VoIP, IP kamera) esetén az átviteli út kismértékű hibája is megakadályozza a szolgáltatás működését (videó rögzítés).

⁹⁶ Electromagnetic Interference

3.5 Az IEEE⁹⁷ 802.11x szabványai [13][14]

Vezeték nélküli elektronikus biztonságtechnikai rendszerek rádiófrekvenciás interfészeinek tervezéséhez, a megfelelő eszközök kiválasztásához elengedhetetlen a rendelkezésre álló, kapcsolódó szabványok, illetve az általuk definiált műszaki paraméterek ismerete, hiszen ezek alapvetően befolyásolják a rendszer képességeit. Ezért az utolsó rész ezek általános megismeréséhez nyújt segítséget.

Az 1997-ben elfogadott eredeti IEEE 802.11 szabvány a frekvenciaugrásos szórt spektrumú (FHSS⁹⁸) és a közvetlen sorrendű szórt spektrumú (DSSS⁹⁹) fizikai réteget tartalmazza, melyek a 2,4 GHz-es frekvencián és 2 Mb/s maximális adatátviteli sebességgel működnek.

Az FHSS maximális sávszélessége már nem elégíti ki a mai igényeket, így nem is használják a WLAN-okhoz, és nem is kompatibilis a 802.11 más alszabványaival. A DSSS már képes együtt működni a 802.11b-vel, de ehhez a szabványhoz ma már nem gyártanak DSSS eszközöket.

3.5.1 IEEE 802.11a

Az IEEE 802.11a szabvány az 1999-es év végén jelent meg. Az 5 GHz-es sávban, 54 Mb/s-os maximális adatátviteli sebességet nyújt, 30 méteres beltéri hatótávon belül.

Ebben a fizikai rétegben működő eszközök nagyrészt 2000 körül kerültek forgalomba. A 802.11a előnye, hogy az 5 GHz-es sáv nincs túltelítve (kevesebb az interferencia, mint a 2,4 GHz-es sávban), és a 12 különálló csatornával a sávszélessége is viszonylag nagy. A hátrányt is az alkalmazott frekvencia körül kell keresni, mert a hatótávolság (30m beltéri, 120m kültéri) korlátait is pont az 5 GHz-es sáv eredményezi. A kis hatótávolság azt eredményezi, hogy ismétlődőket kell alkalmazni a WLAN-ok kiépítésekor.

3.5.2 IEEE 802.11b

A szabvány 1999-ben az IEEE 802.11a szabvánnyal együtt jelent meg. A 802.11a az eredeti szabvány egy nagyobb sebességű változata szintén a 2,4 GHz-es sávra, amely így 11 Mb/s-os adatátviteli sebességet tesz lehetővé.

⁹⁷ Institute of Electrical and Electronics Engineers – Villamosmérnökök és informatikusok nemzetközi szervezete. A világ vezető szakmai non-profit társulata, mely a technológiák fejlesztéséért jött létre 1963-ban.

⁹⁸ Frequency-Hopping Spread Spectrum

⁹⁹ Direct-Sequence Spread Spectrum

A 802.11b hálózati eszközei 1999 óta elérhetőek a kereskedelemben, és ma is szinte minden aktív eszköz támogatja ezt a szabványt. Nagy előnye a hatótávolságban mutatkozik meg, hiszen épületen belül a hatótáv elérheti a 100 métert; hátránya, hogy az eredeti szabvány 14 csatornájából csak 3 (1-es, 6-os, 11-es) csatornát biztosít. A kevés csatornák száma csökkentett hálózati kapacitást eredményez, amit tovább ront a 2,4 GHz-es sáv telítettsége is. Ebben a sávban működik a bluetooth, a mobiltelefonok és a mikrohullámú sütők is, amelyek további interferencia forrást jelentenek. Az interferencia csökkentése miatt használ csak 3 csatornát az eredeti 14 helyett.

A 802.11b szabvány alapvetően két fajta modulációs eljárást alkalmaz. Kisebb adatátviteli sebességhez különbségi bináris fázisbillejtőzést használ (DBPSK¹⁰⁰), nagyobb sebességnél pedig különbségi kvadratúra fázisbillejtőzést (DQPSK¹⁰¹) használ. Ezeknél a modulációknál a fázis eltolásával hoznak létre az adatfolyamban lévő bináris 1-es és 0-k megkülönböztetéséhez jelalakokat.

Ha összehasonlítjuk a 802.11a és b szabványt, akkor arra jutunk, hogy a hatótávolságán belül jóval nagyobb átviteli sebességre képes a 802.11a, míg a hatótávolságán kívül a 802.11b még mindig 1-2 Mb/s-os sebességet tud biztosítani.

Az a és b szabvány inkompatibilitását ellensúlyozva a gyártók több üzemmódú hálózati eszközöket gyártanak. A 802.11a esetében a sebesség függvényében különböző modulációs eljárásokat használnak. 6 Mb/s alatt bináris fázisbillejtőzést (BPSK¹⁰²), felette kvadratúra-amplitúdómodulációt (QAM¹⁰³), ahol a fáziseltolás mellett az amplitúdót is modulálják.

3.5.3 IEEE 802.11g

2003-ban adták ki a 802.11g szabványt, amely a 2,4 GHz-es sávban biztosít maximum 54 Mb/s adatátviteli sebességet, és támogatta a korábbi 802.11b szabvány eszközeit is. A szabvány alapesetben az OFDM¹⁰⁴ modulációs eljárást használja, és a 802.11b-val való kompatibilis működés közben vált DSSS modulációra.

A régebbi szabványokkal való együttműködés fontos az elterjedt 802.11b eszközök miatt, de akkor az elméleti maximális átviteli sebesség 11Mb/s-ra korlátozódik.

¹⁰⁰ Differential Binary Phase Shift Keying

¹⁰¹ Differential Quaternary Phase Shift Keying

¹⁰² Binary Phase Shift Keying

¹⁰³ Quadrature Amplitude Modulation

¹⁰⁴ Orthogonal Frequency-Division Multiplexing

3.5.4 IEEE 802.11i

Bevezetésének célja, hogy korrigálja a korábbi biztonsági problémákat. 2004 nyarán vezették be, és külön kommunikációs, fizikai réteg helyett csak biztonsági előírásokat tartalmaz.

Adattitkosításra az AES¹⁰⁵-t használja és biztonsági szempontból előírja a WPA protokoll használatát.

3.5.5 IEEE 802.11n

A manapság használt vezeték nélküli hálózatok nagy része használja a 2009-ben megjelent 802.11n szabványt, amely a jelenlegi formájában a régi szabványokhoz képest kb. 5-szörös sebességet kínál (elméleti maximuma 600 Mb/s). A sebességnövekedés a MIMO¹⁰⁶ architektúrának köszönhető, amely egy átlagos AP-nál nagyobb területen biztosít ugyanakkora sebességet és sáv szélességet.

A 802.11n egyébként kompatibilis a korábbi 802.11 a/b/g szabványokkal, azaz minden eddigi WiFi eszköz használható az új 802.11n rendszerben, ez semmilyen szoftver vagy hardver változtatást nem igényel.

A 2,4 GHz-es sáv jelenleg túlterhelt, az 5GHz-es viszonylag kihasználatlan. Pont ezt használja ki 802.11n rendszere, amely mindkét frekvenciatartományt egyszerre használja. Az 5 GHz-es sávban 21, a 2,4 GHz-es sávban pedig 3 egymást át nem lapoló csatornát használ a rendszer. A nagy (100 Mb/s feletti) adatátviteli sebesség a csatornák dinamikus felhasználásával lehetséges, amit DF2¹⁰⁷-nek nevezték el.

Az a/b/g hálózatok csak 20 MHz-es, míg a 802.11n hálózatok már 20 MHz és 40 MHz-es sáv szélességgel dolgoztak. A korábbi szabványt alkalmazó rendszereknél problémákat okozott a jel visszaverődés, az n szabvány a többcsatornás átvittel ezt kompenzálja. A MIMO elméleti maximális sebessége 600 Mb/s, amit 4 adó és 4 vevő antennával produkál 4 párhuzamos adatcsatornán.

Ha egy környezetben vizsgáljuk a 802.11 a/b/g és n klienseket, akkor az derül ki, hogy az a/b/g eszközök jobban viselkedtek a 802.11n környezetében, mint a sajátjukban. Vagyis nagyobb teljesítményt érhetünk el, ha a régebbi eszközöket 802.11n hálózatba szervezve használjuk, köszönhetően a MIMO architektúrának.

¹⁰⁵ Advanced Encryption Standard : Szimmetrikus blokk titkosító algoritmust tartalmazó eljárás, 2001-ben vezették be.

¹⁰⁶ Multiple Input, Multiple Output

¹⁰⁷ Dynamic Frequency Selection

Végül talán a legérdekesebb paraméter, a sugárzási tartomány. Megnyugtató, hogy az 5GHz-es tartományban nagyobb, a 2,4 GHz-nél pedig azonos az a/b/g rendszerekkel. Vagyis az AP-k elhelyezése egy az egyben megegyezhet az a/b/g rendszerekkel, sőt ritkábban is elhelyezhetőek a 802.11n AP-k.

A több csatorna egyidejű használata nagyobb bevitt teljesítményt igényel, ami azt jelenti, hogy a 802.3af¹⁰⁸ szabvány által előírtnál (12,9W) nagyobb teljesítményű eszközökre van szükség. A 802.3af+ már tartalmazza a nagyobb teljesítményű AP-k táplálására vonatkozó követelményeket.

¹⁰⁸ A tápfeszültség Ethernet hálózaton való szállításáról szóló szabvány (PoE - **P**ower **o**ver **E**thernet).

4 **Összefoglalás**

Az elektronikus biztonságtechnikai rendszereknél alkalmazott vezeték nélküli megoldások körültekintő tervezés esetén megfelelő védelmet biztosítva képesek megbízhatóan üzemelni. Ugyanakkor lehetnek olyan, elsősorban katonai, illetve nemzetbiztonsági célú alkalmazások, ahol kvázi zérus maradék kockázatra szükséges törekedni, ezért nem megengedhető a vezeték nélküli technológiák alkalmazása.

A vezeték nélküli rendszerek alapvető jellemzőikből adódóan más biztonsági jellemzőkkel rendelkeznek, mint vezetékes társaik. Az átviteli közeg a levegő, ahol az alkalmazott antennák karakterisztikájától függően akár a tér minden irányába kisugárzódhat az átvinni kívánt rádiófrekvenciás jel. Természetesen a szükséges adminisztratív és műszaki eljárások, technológiák alkalmazásával, valamint megfelelő védelmi intézkedések bevezetésével és betartásával elérhető, hogy ne jelentsen lényegesen nagyobb kockázatot egy rádiófrekvenciás, mint egy vezetékes realizáció.

Gyakran találkozhatunk olyan körülményekkel, amelyek ismeretében már a tervezési fázis elején el kell vetni az adott vezeték nélküli eszköz alkalmazását, mert egyszerűen nem felel meg az elvárt követelményeknek. A szakmai gyakorlatom során megismert eszközök között volt olyan vagyonvédelmi központ, amely az általános 433 MHz-es rádiós átvittel csatlakozó mozgásérzékelő szabotázst gyakorlatilag nem érzékelte. Ez nem a rádiófrekvenciás interfész technológiai hiányosságára volt visszavezethető, hanem a központot vezérlő szoftver programozói hibájára. Több, a kereskedelemben kapható rendszernél is fellép hasonló jelenség, ami a vezeték nélküli végpontok meghatározott időközönként történő bejelentkezésének rendszerével, illetve annak hiányosságaival hozható összefüggésbe. A hasonló problémák elkerülhetőek olyan berendezések alkalmazásával, amelyeket az egyéni igényeknek megfelelően alakítottak ki. A rendellenes működésből eredő kockázat csökkenthető, ha adott rendszerre optimalizált egyedi vezérlőszoftvereket alkalmazunk.

A vezeték nélküli rendszerek legnagyobb előnye a rugalmasságukban rejlik, hiszen akár a folyamatosan változó körülményekhez és követelményekhez gyorsan, költséghatékonyan, jelentős átalakítások nélkül alkalmazkodni képes megoldások hozhatók létre végpontok

cseréjével, áthelyezésével, új szenzorok rendszerbe integrálásával, ami akár a védett terület, akár a védelmi képesség utólagos kiterjesztését is lehetővé teszi.

Irodalomjegyzék

- [1] Dr. Kiss Sándor: Biztonságtechnika alapja, főiskolai jegyzet (ZMNE, 2004)
- [2] Dr. Lukácsi György (és mások): Új vagyonvédelmi nagykönyv (CEDIT Kft., 2002)
- [3] Laczkó Gábor: A biometria alapjai (<http://securinfo.hu/termekek/biometria/760-a-biometria-alapjai.html>, letöltve: 2012.04.13)
- [4] Általános biometriai szakkifejezések szószedete (<http://biolock.hu/w3/dict.shtml>, letöltve: 2012.04.11)
- [5] Istvánffy Edvin: Tápvonalak, antennák és hullámterjedés (Műegyetemi Kiadó, 1997)
- [6] Online függvényábrázoló alkalmazás (<http://fooplot.com>, letöltve: 2012.04.07)
- [7] Gunnar Heine: GSM networks: protocols, terminology, and implementation (<http://www.supcom.mincom.tn/~ridha/6tel/docs/Artech.House,.GSM.Networks.Protocols.Terminology.and.Implementation.pdf>, letöltve: 2012.03.31)
- [8] Lázár Zoltán, Dr. Eged Bertlan: Bluetooth (BME, Mikrohullámú Híradástechnika Tanszék, 2000)
- [9] Jim Geier (fordította: Harangozó Gábor): Vezeték nélküli hálózatok (Panem Kft., 2005)
- [10] Tom Thomas: Hálózati biztonság (Panem Kiadó, 2005)
- [11] Merritt Maxim, David Pollino: Wireless Security (The McGraw-Hill Companies, 2002)
- [12] Laurett Butti, Julien Tinnès: Discovering and exploiting 802.11 wireless driver vulnerabilities (J Comput Virol, 2008, 4(1), 25-37)
- [13] Matthew S. Gast: 802.11 Wireless Networks: The Definitive Guide (O'Reilly Media, 2005)
- [14] Joseph Davies: Biztonságos vezeték nélküli hálózatok (Szak Kiadó Kft., 2005)

Ábrajegyzék

1. ábra: A komplex védelem értelmezése
2. ábra: Az ún. NATO-drót szerkezete
(forrás: http://oktel.hu/wp-content/uploads/2010/12/NATO_kerites_s.jpg,
letöltve: 2012.04.12.)
3. ábra: Reed relé
(forrás: http://ob121.com/hard_sensor.html#reed_rele,
letöltve: 2012.04.12.)
4. ábra: Néhány biometrikus rendszer FAR mutatója
(forrás: <http://oktel.hu/>)
5. ábra: A biztonságtechnikában alkalmazott néhány VHF, UHF frekvenciatartomány
6. ábra: Interferencia jelenség két szélsőséges esetben
(forrás: <http://fooplot.com>, letöltve: 2012.04.07)
7. ábra: Átvitel szabadtéri lézerrel
(forrás: <http://www.digitalairwireless.com/images/pageimages/laser-links.jpg>,
letöltve: 2012.04.21.)
8. ábra: Kismet alkalmazás
(forrás: http://openmaniak.com/kismet_conf.php,
letöltve: 2012.04.01.)
9. ábra: „WOK WiFi”
(forrás: <http://i44.tinypic.com/2u9n6gh.jpg>,
letöltve: 2012.04.07.)
10. ábra: A lefedettség megjelenítése az AirMagnet Surveyor Pro segítségével
(forrás: <http://www.cisco.com/en/US/i/200001-300000/220001-230000/222001-223000/222901.jpg>,
letöltve: 2012.04.09.)

Rövidítésjegyzék

ACL	Access Control List (hozzáférés vezérlő listák)
AES	Advanced Encryption Standard (fejlett titkosítási szabvány)
AP	Access Point (hozzáférési pont)
ARP	Address Resolution Protocol (címfeloldó protokoll)
BPSK	Binary Phase Shift Keying (kétállapotú fázisbillentyűzés)
CCD	Charge-Coupled Device (töltés-csatolt eszköz)
CCTV	Closed Circuit TeleVision (zártláncú televízió)
CMOS	Complementary Metal-Oxide Semiconductor (komplementer fém-oxid félvezető)
DBPSK	Differential Binary Phase Shift Keying (differenciál kétállapotú fázisbillentyűzés)
DDoS	Distributed Denial of Service (elosztott szolgáltatás megtagadása)
DFS	Dynamic Frequency Selection (dinamikus frekvencia-kiválasztás)
DHCP	Dynamic Host Configuration Protocol (dinamikus állomáskonfiguráló protokoll)
DoS	Denial of Service (szolgáltatásmegtagadással járó támadás)
DQPSK	Differential Quaternary Phase Shift Keying (differenciál négyállapotú fázisbillentyűzés)
DSP	Digital Signal Processing (digitális jelfeldolgozás)
DSSS	Direct-Sequence Spread Spectrum (direkt szekvenciás szórt spektrum)
EMI	Electromagnetic Interference (elektromágneses interferencia)
FAR	False Acceptance Ratio (téves elfogadási hányad)
FHSS	Frequency-Hopping Spread Spectrum (frekvenciaugratásos szórt spektrum)
FOIDS	Fiber Optic Intelligence & Detection System (üvegszálás felderítő és érzékelő rendszer)
FSO	Free Space Optics (szabad téri optika)
GFSK	Gaussian Frequency Shift Keying (Gauss frekvenciaeltolásos billentyűzés)
GPRS	General Packet Radio Service (csomagkapcsolt mobil átviteli technológia)
GSM	Global System for Mobile Communications

	(globális mobil kommunikációs rendszer)
GYODA	Gyorsan telepíthető drótkadály
IDS	Intrusion Detection System (behatolás érzékelő rendszer)
IMSI	International Mobile Subscriber Identity (nemzetközi mobil előfizető azonosító)
IP	Internet Protocol
ISM	Instrumentation, Scientific, and Medical band (műszeres, tudományos és orvosi sáv)
Kc	Cipher Key (titkosítási kulcs)
Ki	Individual Subscriber Authentication Key (személyleíró hitelesítő kulcs)
LFSR	Linear Feedback Shift Register (lineáris visszacsatolt shiftregiszter)
MAC	Media Access Control (közegelés vezérlés)
MAD	Magnetic Anomaly Detection (mágneses anomália detektálás)
MIMO	Multiple Input, Multiple Output (többszörös bemenet, többszörös kimenet)
OFDM	Orthogonal Frequency-Division Multiplexing (kódolt ortogonális frekvenciaosztásos multiplexálás)
PIN	Personal Identification Number (személyi azonosító szám)
PIR	Passive InfraRed (passzív infravörös)
PUK	PIN Unblock Key (PIN feloldó kulcs)
QAM	Quadrature Amplitude Modulation (kvadratúra amplitúdómoduláció)
RFID	Radio Frequency IDentification (rádiófrekvenciás azonosítás)
ROI	Return on Investment (várható megtérülés)
SARP	Secure ARP (biztonságos címfeloldó protokoll)
SIM	Subscriber Identity Module (előfizetői azonosító egység)
SMS	Short Message Service (rövid szöveges üzenet szolgáltatás)
SRD	Short Range Devices (kis hatótávolságú eszközök)
SRES	Signed Response (aláírt válasz)
SSID	Service Set Identifier (szolgáltatáskészlet-azonosító)
TMSI	Temporary Mobile Subscriber Identity (ideiglenes mozgó előfizetői azonosító)
UHF	Ultra High Frequency (deciméteres hullám)
UMTS	Universal Mobile Telecommunications System (általános mobil telekommunikációs rendszer)
VHF	Very High Frequency (ultrarövidhullám)
VoIP	Voice over IP (IP telefónia)

VPN	Virtual Private Network (virtuális magánhálózat)
WEP	Wired Equivalency Policy (vezetékeskel egyenértékű (biztonságú) hálózat)
WLAN	Wireless Local Area Network (vezeték nélküli helyi hálózat)
WPA	Wi-Fi Protected Access (Wi-Fi védett hozzáférés)
XOR	„kizáró vagy” logikai művelet