Centar Informacijske Sigurnosti

Ometanje signala bežičnih mreža

lipanj 2011.

CIS-DOC-2011-08-023

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

U današnje vrijeme postoji jako veliki broj mreža. Mreže se dijele u dvije osnovne skupine: žične i bežične mreže. Žične mreže su sigurnije od bežičnih zbog toga što napadač mora biti fizički povezan s odašiljačem/prijemnikom ili žicom koja prenosi signale između njih. Kod bežičnih mreža nema takvih ograničenja, tj. napadač može izvesti svoj napad i s većih udaljenosti koristeći samo radiovalove. Ipak bežične mreže su sve češće i javljaju se u različitim oblicima. Primamljive su jer omogućuju jednostavniji rad, lakšu povezanost, a korisnici mogu koristiti usluge bilo gdje jer ne moraju tražiti priključak na koji bi spojili svoj uređaj

Tehnologije koje svakodnevno koristimo poput WLAN-a (eng. *Wireless Local Area Network*), mobilne telefonije i televizije koriste radiovalove za prijenos informacija. Podaci koji se prenose na takav način nisu zaštićeni kao podaci koji se prenose žicama pa su bežične mreže česta meta napadača.

Jedan od čestih oblika napada na bežične mreže je izvođenje DoS (eng. *Denial of Service*) napada. Ovaj napad je najjednostavnije izvesti korištenjem uređaja za ometanje bežičnih mreža, popularno zvanih *jammeri*. Oni se najčešće koriste za ometanje WLAN mreža i signala mobilnih telefona pa je u ovom dokumentu veći naglasak stavljen na ove dvije bežične tehnologije.

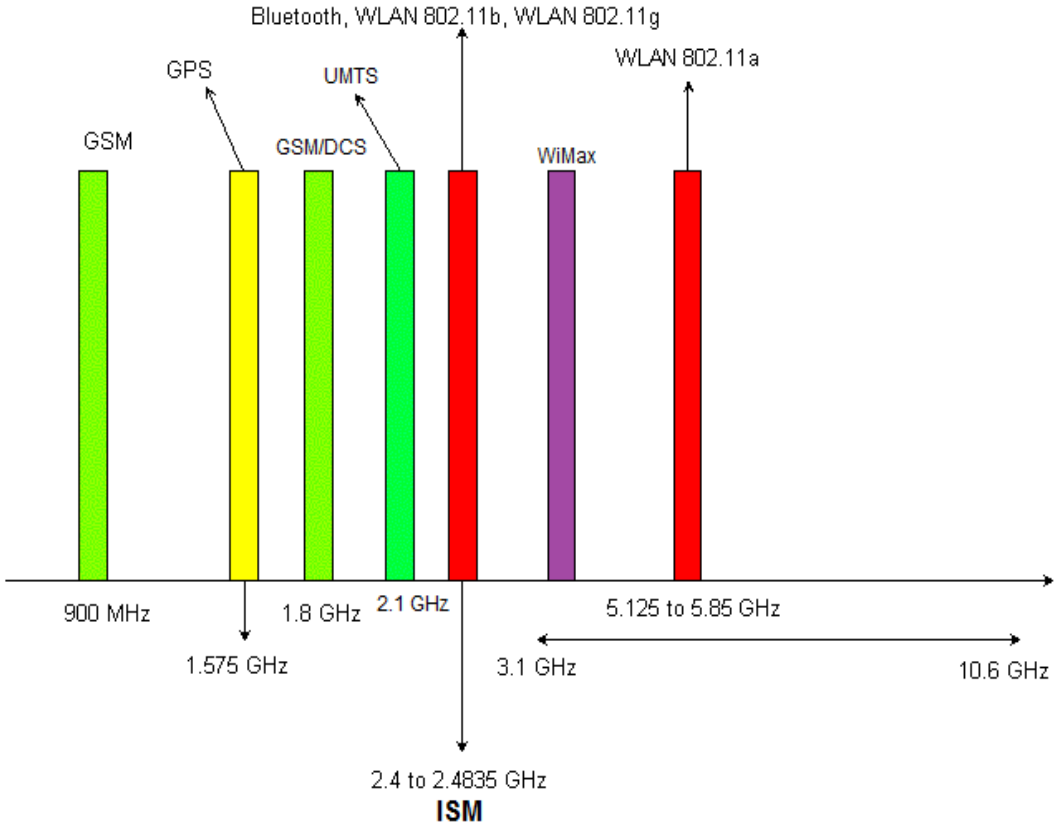
Prvo poglavlje opisuje neke osnovne pojmove vezane uz bežičnu tehnologiju kako bi se lakše shvatilo kako rade uređaji za ometanje bežičnih mreža. U drugom poglavlju se opisuje što je potrebno za uspješno ometanje i na koje načine je moguće izvesti ometanje. Zadnje poglavlje opisuje neke tehnike koje su razvijene kako bi se umanjile posljedice ometanja signala.

2. Bežične mreže

Bežične mreže su mreže kod kojih se podaci prenose radiovalovima zbog čega nije potrebno uređaje povezivati kablovima. Najpoznatiji primjeri mreža koje koriste radiovalove za prijenos informacija su WLAN, mobilna telefonija, zemaljska i satelitska televizija te bežični širokopojasni pristup Internetu (WiMax). U ovom dokumentu opisati će se detaljnije mobilna telefonija i WLAN mreže te način na koje se one ometaju budući da su upravo one najčešća meta napada.

2.1. Frekvencijski pojasevi

Radiovalovi koji prijenose informacije mogu raditi na raznim frekvencijama iz radiofrekvencijskog spektra, a frekvencije se kreću između 3 kHz i 300 GHz. Frekvencija na kojoj će uređaji raditi ovisi o zahtjevima pojedine tehnologije. Na primjer, frekvencije oko 24.5 GHz omogućuju veće brzine prijenosa, ali udaljenost između odašiljača i prijemnika je manja nego na frekvencijama oko 3.5 GHz. Bežične mreže su jako osjetljive na interferenciju radiovalova do koje može doći ako dvije različite bežične mreže prenose različite podatke na istoj frekvenciji. U tom slučaju se pojavljuju smetnje i signal postaje toliko izobličen da obje bežične mreže ne mogu više prenositi podatke. Kako bi se izbjegla interferencija, potrebno je različitim bežičnim mrežama dodijeliti različite frekvencije. Dodjeljivanjem frekvencija iz radiofrekvencijskog spektra upravlja organizacija ITU [1](eng. *International Telecommunication Union*). Svakoj bežičnoj tehnologiji je dodijeljen točno određeni frekvencijski pojas (slika 1).



Slika 1. Podjela radiofrekvencijskog spektra
Izvor: www.educypedia.be

[1] ITU je organizacija unutar Ujedinjenih Naroda, a odgovorna je za informacijske i komunikacijske tehnologije. ITU upravlja radiofrekvencijskim spektrom, standardizacijom opreme i razvojem informacijske i komunikacijske tehnologije.

Na primjer, WLAN mreže po 802.11 standardu (Wi-Fi mreže) rade u rasponu od 2400 do 2483 MHz, a mobilni telefoni treće generacije (3G mreže koje koriste UMTS) u Europi koriste frekvencije oko 2100 MHz (od 2110 do 2170 MHz). Raspodjela frekvencija za pojedine tehnologije se razlikuje ovisno o državi. Na primjer, spomenute 3G mreže u Hrvatskoj koriste frekvencije od 2110 do 2170 MHz dok u SAD-u koriste frekvencije između 1930 i 1990 MHz. U tablici 1 su prikazane frekvencijski pojasevi za mobilnu telefoniju i WLAN mreže u Hrvatskoj.

Tehnologija	Frekvencijski pojas [MHz]
WLAN (Wi-Fi)	2400 - 2483.5
GSM	Silazno: 925 - 960 Uzlazno: 880 - 915
GSM/DSC	Silazno: 1805 - 1880 Uzlazno: 1710 - 1785
UMTS	Silazno: 2110 - 2170 Uzlazno: 1920 - 1980

Tablica 1. Frekvencijski pojasevi za WLAN i mobilnu telefoniju u Hrvatskoj

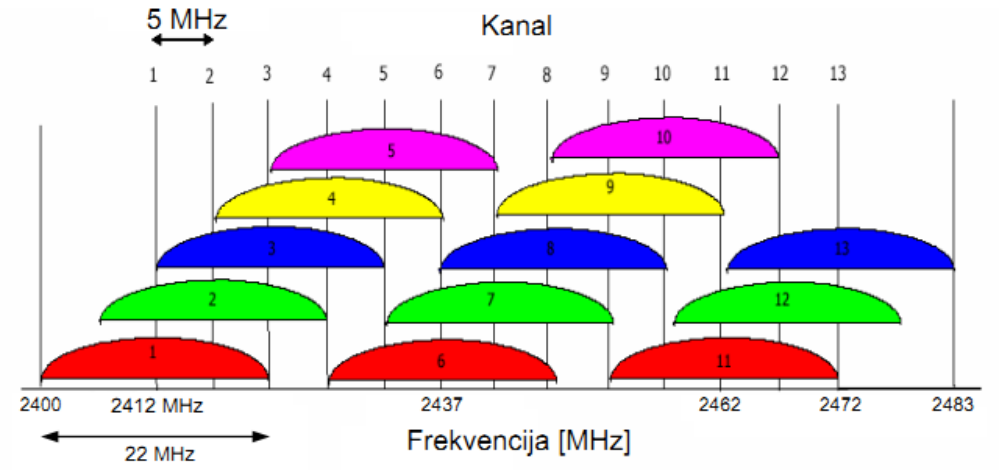
Većina frekvencijskih pojaseva se naplaćuje, ali postoji par malih frekvencijskih pojasa koji su besplatni za korištenje. Jedan takav pojas se nalazi oko 2.4 GHz i zove se ISM[2] (eng. *industrial, scientific and medical*) frekvencijski pojas. U Europi je taj pojas širine 83.5 MHz, a koriste ga brojne poznate bežične tehnologije poput Wi-Fi (eng. *Wireless-Fidelity*), Blueetooth i kućnih bežičnih telefona. WLAN mreže koje koriste ISM pojas su poznate pod imenom Wi-Fi, a zapravo se radi o mrežama koje se pridržavaju 802.11b/g/n standarda. Skup normi 802.11 uključuje i 802.11a normu koja se također koristi za bežični pristup Internetu, ali umjesto 2.4 GHz koristi pojas na 5 GHz te nije sukladna s normama 802.11b/g/n.

Ostali frekvencijski pojasevi navedeni u tablici 1 koriste se za mobilnu telefoniju. Može se primijetiti da mobiteli za razliku od Wi-Fi uređaja koriste tri frekvencije za rad. Prvi skup frekvencija koji se koristio još u vrijeme GSM (eng. *Global System for Mobile Communications*) mobitela je onaj na 900 MHz, a daljnjim razvojem mobilne telefonije, uvođenjem novih tehnologija i prelaskom na 3G mreže, radiofrekvencijski spektar kojeg koriste mobilni telefoni se povećao. U tablici su za svaku tehnologiju mobilne telefonije navedene dvije skupine frekvencijskih pojaseva: jedan za silaznu i jedan za uzlazni vezu. Naime, mobilni telefoni rade u *full-duplex* načinu rada, što znači da koriste različite frekvencije za primanje i slanje podataka. Skup frekvencija za silaznu vezu koriste bazne stanice kada šalju podatke do mobilnih uređaja, a skup frekvencija za uzlaznu vezu koriste mobilni uređaji pri svom slanju podataka. Zbog *full-duplex* načina rada, mobiteli mogu istovremeno i primati i slati podatke (obje strane telefonskog razgovora mogu istodobno pričati).

2.2. Kanali

Kako bi se dodijeljeni frekvencijski pojas što bolje iskoristio, on se dijeli u kanale. Kanale čini raspon od nekoliko frekvencija u dodijeljenom frekvencijskom pojasu. Pojedini uređaj prenosi podatke koristeći samo jedan kanal, a ne cijeli pojas. Tako više uređaja koji koriste istu tehnologiju može istovremeno raditi čak i kada se nalaze blizu jedan drugom. Na primjer, ISM pojas na 2.4 GHz u Europi podijeljen je na 13 kanala širine 22 MHz kao na slici 2. U Americi je taj pojas nešto uži pa je zbog toga podijeljen na 11 kanala.

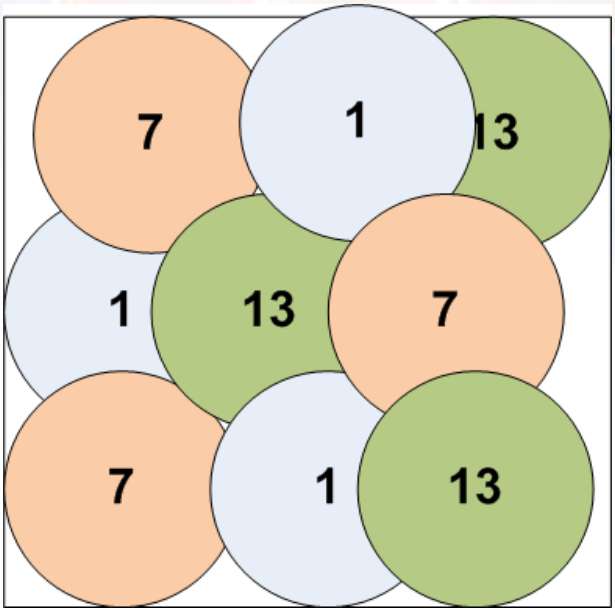
[2] ISM pojaseve je definirala organizacija ITU, a namijenjeni su za korištenje u industrijske, znanstvene i medicinske svrhe. Većina ISM pojasa je relativno uska, tek nekoliko desetaka ili stotina MHz, a najpoznatiji je ISM pojas na 2.4 GHz.



Slika 2. Podjela ISM pojasa na kanale za WLAN
Izvor: zrk.fer.hr

Iako se na prvi pogled čini da je 13 kanala i više nego dovoljno za rad, boljim promatranjem slike 2 može se otkriti zašto se nikada ne koristi svih 13 kanala. Naime, kanali se preklapaju i istovremenim korištenjem, primjerice, kanala 1 i 2 dolazi do velike interferencije što rezultira jako velikim brojem izgubljenih paketa pri slanju podataka. Zbog toga se rijetko kada koriste više od tri kanala. Kanali koji se u Europi koriste za Wi-Fi mreže su kanali 1, 7 i 13 koji su međusobno dovoljno razmaknuti da ne uzrokuju interferenciju.

Činjenicu da postoje samo tri upotrebljiva kanala treba uzeti u obzir kod projektiranja WLAN mreža. Ova bežična mreža se sastoji od uređaja koji se zovu pristupne točke. Oni odašilju i primaju bežične signale do i od ostalih WiFi uređaja i tako omogućuju, primjerice, bežično spajanje prijenosnog računala na Internet. Kada treba pokriti veće površine, koristi se više pristupnih točki čije se područje prekrivanja na nekim mjestima preklapa. Svaka pristupna točka koristi jedan od tri moguća kanala što znači da pristupne točke s kojima se preklapa moraju koristiti druge kanale (slika 3). U suprotnom, dolazilo bi do interferencija na mjestima preklapanja.



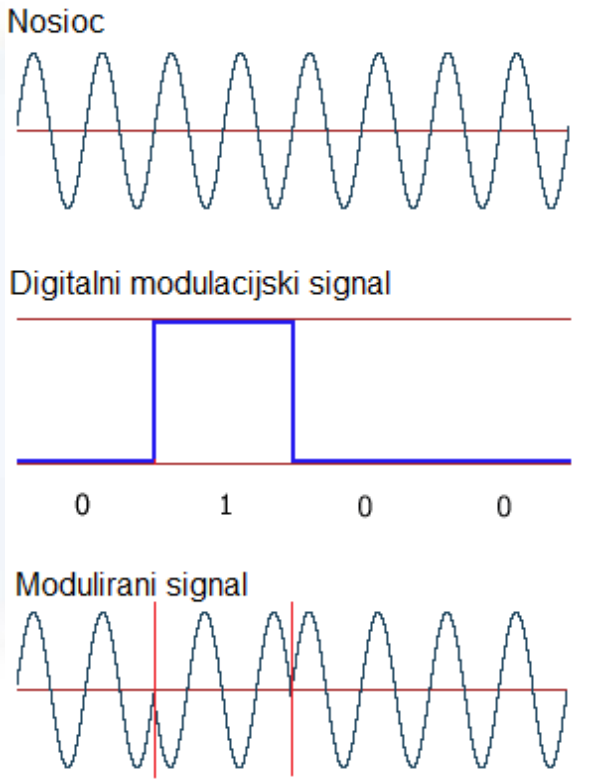
Slika 3. Primjer planiranja pokrivenosti WLAN mreže
Izvor: LSS

Kod mobilne telefonije podjela frekvencijskog pojasa na kanale i njihova upotreba ovisi o tehnologiji koja se koristi i broju korisnika koji ih žele koristiti.

2.3. Prijenos podataka

Do sada je objašnjeno da se radiofrekvencijski spektar dijeli u frekvencijske pojaseve koji se dodjeljuju pojedinoj tehnologiji, a frekvencijski pojasevi se dijele u kanale koje uređaji koriste pri prijenosu podataka. Sam prijenos podataka opisan je u nastavku dokumenta.

Podaci koji se prenose su digitalizirani, tj. radi se o nizu nula i jedinica. Postupkom modulacije se podaci iz modulacijskog signala upisuju u signal nosioc koji je najčešće sinusni signal (slika 4). Modulacijom se nosiocu mijenjaju parametri (amplituda, faza i/ili frekvencija) ovisno o podacima koji se žele prenijeti. Rezultat modulacije je modulirani signal koji se odašilje. U primjeru na slici 4 izvodi se binarna diskretna modulacija faze ili BPSK [3](eng. *Binary phase shift keying*). Ako se prenosi bit 0, onda se signal nosioc ne mijenja, a ako se prenosi 1, signal nosioc ima skok u fazi. Na prijemnoj strani se izvodi obrnuti postupak demodulacije kojim se iz moduliranog signala dobivaju nizovi nula i jedinica. Neki postupci modulacije su osjetljiviji na greške od drugih. Primjer modulacije na slici 4 je jedan od najrobusnijih, ali zato ostvaruje manje brzine prijenosa. BPSK modulacija se koristi kada je potrebno osigurati veliku točnost pri bežičnom prijenosu (npr. vojne komunikacije) ili kada je interferencija u kanalu jako velika kako bi se smanjila vjerojatnost greške.



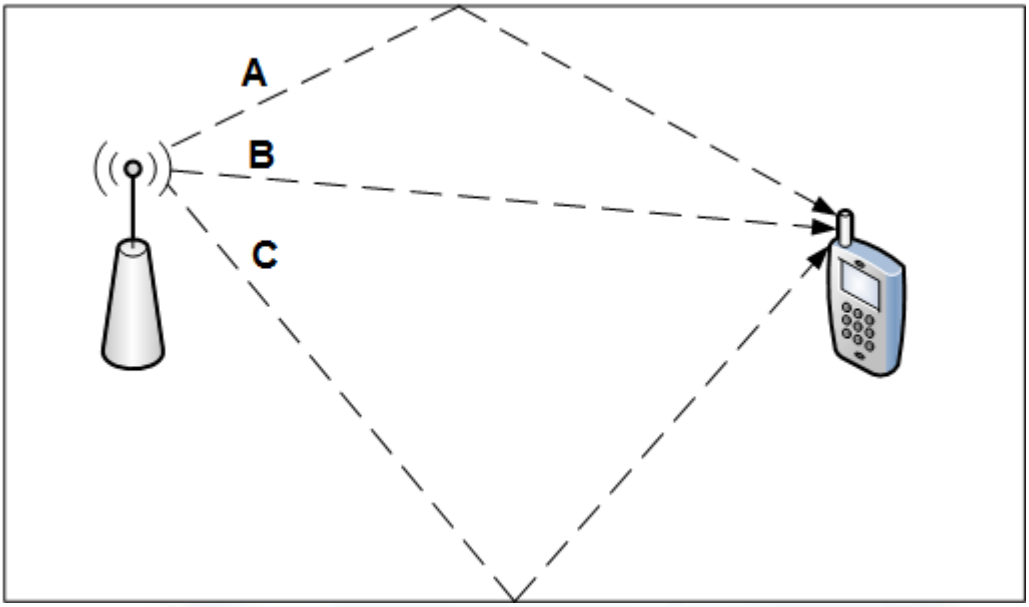
Slika 4. Diskretna modulacija faze
Izvor: www.ustudy.in

Osim BPSK, postoje QPSK (eng. *Quadrature phase-shift keying*) i 8-PSK modulacijski postupci koji također mijenjaju faznu vrijednost signala nosioca, ali umjesto samo dva stanja faze (0° i 180° u BPSK) koriste četiri (0°, 90°, 180° i 270° u QPSK) ili osam stanja faze (8-PSK). Što se više stanja faze koristi, to je veća brzina prijenosa, ali i veća osjetljivost na pogreške. Modulacijski postupci koje mijenjaju frekvencijsku vrijednost signala nosioca se zovu M-FSK (eng. *M Frequency-shift keying*), gdje je M broj stanja frekvencije (M je potencija broja dva). Veće brzine prijenosa podržavaju one modulacijske tehnike s većom vrijednosti M. Za frekvencijske modulacije vrijedi isto što i za fazne: što je veća brzina prijenosa, to je veća osjetljivost na

[3] BPSK je jedan oblik modulacijskog postupka kod kojeg se signalu nosiocu mijenja fazna vrijednost ovisno o binarnim podacima koji se žele prenijeti. Ako je vrijednost binarnog podatka 0, onda se fazna vrijednost ne mijenja, a ako je vrijednost 1, onda fazna vrijednost ima skok za 180°.

pogreške. Još jedan vrlo često korišteni modulacijski postupak je QAM (eng. *Quadrature amplitude modulation*). Ovaj postupak mijenja dva parametra signala nosioca: amplitudu i fazu. Inačice QAM postupka koje se koriste su: 4-QAM, 16-QAM, 64-QAM i 256-QAM. Čak i kod pažljivog korištenja frekvencijskih kanala, moguće su interferencije. Na primjer, poslani signal može interferirati sam sa sobom.

Na slici 5 prikazan su odašiljač radiosignala i mobilni uređaj koji prima taj signal. I odašiljač i prijamnik se nalaze u zatvorenoj sobi. Odašiljač emitira radiovalove u svim smjerovima. Neki valovi izravno dolaze do prijemnika u mobilnom uređaju (zraka B), dok neki valovi dolaze do prijemnika refleksijom na zidovima prostorije (zrake A i C). Zraka B najbrže dolazi do prijemnika, a zrake A i C dolaze s vremenskim kašnjenjem. Prijemnik ne zna da sve zrake nose iste informacije pa ih sve uzima u obzir. Ove tri zrake međusobno interferiraju i mogu uzrokovati gušenje ili izobličenje signala. Ova pojava se zove višestazno prostiranje, a rješava se uvođenjem zaštitnog razmaka, kompenziranjem utjecaja okoline kroz koju signal prolazi, dodavanje zaštitnih bitova koji omogućuju ispravljanje grešaka itd. Ove metode također smanjuju posljedice namjernog ometanja signala bežičnih mreža. Npr. ukoliko se ometanjem signal izobliči, ove tehnike ga ipak mogu ispraviti.



Slika 5. Višestazno prostiranje
Izvor: LSS

Još jedan oblik zaštite bežičnih signala su tehnike proširenog spektra poput:

- postupka s izravnim slijedom ili DSSS (eng. *Direct Sequence Spread Spectrum*) i
- postupka sa skakanjem frekvencije ili FHSS (eng. *Frequency Hopping Spread Spectrum*).

Prošireni spektar je sredstvo prijenosa kod kojeg signal zauzima veću širinu pojasa od najmanje potrebne za slanje informacija. Širenje spektra postiže se pomoću koda koji je neovisan o podacima te sinkroniziranim prijemom koda na prijemniku za širenje spektra i izvlačenje informacije. Tehnike proširenog spektra se koriste kao zaštita od smetnji (interferencija), zaštita od prisluškivanja i zaštita od ometanja. Prošireni spektar podrazumijeva korištenje velikog spektra za svaki prijenos, što se kompenzira smanjenjem smetnji i većim brojem korisnika koji koriste isti spektar. Tehnike proširenog spektra su detaljnije objašnjene u poglavlju 4.1.

Jedna od vrlo važnih mjera u bežičnom prijenosu je omjer signala i šuma ili SNR (eng. *Signal to noise ratio*) koji se računa prema sljedećem izrazu:

$$SNR = 10\log_{10}\frac{P_{signal}}{P_{šum}}$$

SNR zapravo računa omjer snage signala i snage šuma u decibelima. Što je SNR veći, to će komunikacija biti uspješnija jer velik SNR znači da šum ne može nadjačati signal. Šum su sve smetnje koje ometaju prijenos. On može biti prirodni šum koji uvijek postoji, šum od interferencije, ali i namjerno emitirani šum kojem je cilj onemogućiti prijenos podataka (npr. šum koji emitiraju uređaji za ometanje bežičnih mreža).

3. Ometanje bežičnih mreža

Ometanje signala bežičnih mreža (eng. *radio jamming*) se izvodi emitiranjem posebnog radio signala (eng. *jamming signal*) koji će stvoriti interferenciju sa signalom kojeg se želi ometati i smanjiti odnos signal/šum. Za ometanje bežičnih mreža ključne su tri stvari:

1. Signal za ometanje mora se emitirati na **istoj frekvenciji** kao signal bežične mreže.
2. Signal za ometanje mora biti **moduliran na isti način** kao signal bežične mreže.
3. Signal za ometanje mora **imati veću snagu** od signala bežične mreže.

Cilj ometanja signala bežičnih mreža je izvesti DoS [4](eng. *Denial of Service*) napad. U tom slučaju je ometanje toliko jako da potpuno onemogućuje bilo kakvu komunikaciju preko napadnute bežične mreže. Ipak, nekada je i djelomično ometanje dovoljno jer otežava komunikaciju (npr. dovoljno je omesti 30% govorne poruke da ona postane nerazumljiva).

3.1. Povijest

Ometanje signala bežičnih mreža se koristilo još u Drugom svjetskom radu. Tada su se ometali neprijateljski radari i radio stanice, a cilj je bio onemogućiti komunikaciju neprijatelja. Kao način obrane od ovakvih napada koristile su se tehnike proširenog spektra, a radio stanice su često pojačavale snagu emitiranja i mijenjale frekvenciju na kojoj emitiraju program.

Ometanje radio signala se koristilo i u kasnijim ratovima u Izraelu, Kubi, Iraku, Iranu, Kini, Sjevernoj i Južnoj Koreji itd. U razdoblju hladnog rata istočne i zapadne sile su postavile brojne odašiljače signala za ometanje kako bi onemogućile komunikaciju i emitiranje radio programa neprijateljskih strana. Ometanje se sprječavalo povećanjem snage odašiljanja, upotrebom usmjerenih antena (antene koje emitiraju samo u jednom smjeru) i korištenjem dodatnih frekvencija za emitiranje. Ovakav način borbe protiv ometanja signala doveo je do dodatnih problema zbog kojih su ometanje trpile i radio stanice koje nisu bile meta poput vlastitih radio stanica. SSSR (Savez Sovjetskih Socijalističkih Republika) i istočna Njemačka su ometali gotovo sve veće zapadne radio stanice. Slušatelji u tim područjima su koristili antenske petlje (kružne antene) koje su omogućavale prijem radio stanice unatoč velikom šumu. Budući da na propagaciju radio valova utječu brojni faktori poput atmosferskih uvjeta, ometanje signala nije bilo moguće uvijek ostvariti pa su u tim rijetkim razdobljima slušatelji ipak mogli čuti inače ometane radio stanice. Sovjeti su koristili dva tipa odašiljača signala za ometanje. Jedan je pokrivao veća područja, ali su na njegovu učinkovitost jako utjecali vremenski uvjeti. Drugi tip odašiljača je pokrivao manja područja i koristio se u većim gradovima.

Ometanje radio stanica se koristi i danas. Kina blokira emitiranje svih stranih radio stanica od 2002. godine kako bi ograničili pristup informacijama iz drugih država. Iran često ometa signale satelitske televizije, a jedno od takvih ometanja je bilo 2009. godine kada se pokušalo spriječiti širenje informacija o prosvjedima. Sjeverna i Južna Koreja redovito međusobno ometaju radio i televizijske signale.

Danas kada se govori o ometanju bežičnih mreža, najčešće se misli na ometanje mobilne telefonije i WLAN mreža. Zbog toga je u ovom dokumentu najveći naglasak stavljen na ove dvije bežične mreže.

[4] DoS napad radi na principu opterećivanja određenog resursa sve dok resurs postane nedostupan.

3.2. Nenamjerno ometanje bežičnih mreža

Nisu sva ometanja bežičnih mreža namjerna. Do ometanja neke radio stanice može doći ukoliko druga radio stanica emitira svoj signal bez da je prije provjerila koristi li se ta frekvencija. Ipak, do ovakvog ometanja u pravilu ne dolazi zbog toga što je korištenje radiofrekvencijskog spektra strogo regulirano. ITU se brine o dodjeli radiofrekvencijskog spektra tako da svaka tehnologija koristi točno određeni dio spektra i smeta radu ostalih. Ako dođe do ovakvog ometanja, ITU može zaustaviti ometača.

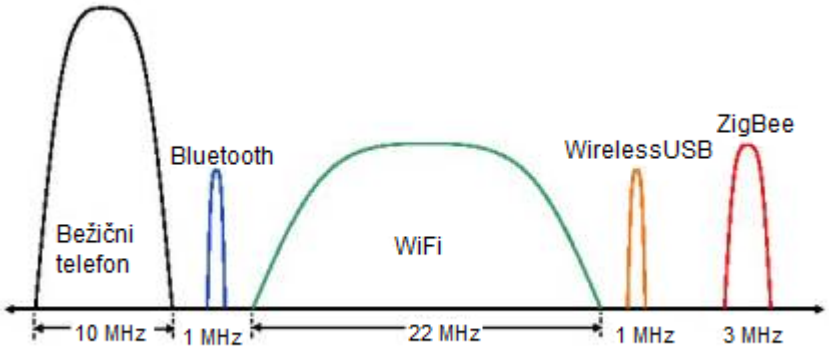
Na širenje radiovalova i kvalitetu prijema utječu atmosferske prilike i prepreke poput zidova, zgrada i drveća. Smetnje u mobilnoj telefoniji nekada mogu uzrokovati atmosferske neprilike. Ipak, ovi faktori se uzimaju u obzir pri projektiranju bežičnih mreža, tako da rijetko dolazi do ometanja signala na ovaj način.

Još jedan nenamjerni oblik ometanja bežičnog signala je kada neki uređaj (poput mikrovalne pećnice) emitira radiovalove tijekom svog rada. Ovisno o frekvenciji na kojoj titraju emitirani valovi, postoji mogućnost interferencije s nekom bežičnom mrežom. Mikrovalna pećnica radi na 2.45 GHz i može ometati signal Wi-Fi pristupne točke koja radi na 2.4 GHz. Postojanje ovakvog ometanja je dobro poznato i treba uzeti u obzir pri postavljanju pristupne točke poput kućnog Wi-Fi usmjerivača. WLAN mreža interferira s drugim uređajima koji rade u području 2.4 GHz, a tih uređaja ima puno budući da se radi o ISM frekvencijskom području za kojeg nije potrebno plaćati naknadu. Još neki od uređaja koji rade u području od 2.4 GHz su:

- kućni bežični telefoni,
- Bluetooth uređaji,
- bežični USB (*WirelessUSB*) i
- ZigBee uređaji.

U nastavku će se objasniti spomenuti uređaji i način na koji oni koriste ISM frekvencijski pojas.

Na slici 6 su prikazane širine kanala koje uređaji u pojasu od 2.4 GHz zauzimaju. Ovisno o tome gdje su uređaji postavljeni i kako se koriste moguće su veće ili manje interferencije. Kućni bežični telefoni koji rade na frekvenciji od 900 MHz ili 5.8 GHz neće uzrokovati interferencije, ali oni modeli koji rade na frekvenciji od 2.4 GHz mogu nadjačati Wi-Fi signal i tako ometati rad bežične mreže. Pogledom na sliku 6 jasno je zašto bežični telefon može jako utjecati na rad Wi-Fi mreže. Kanal koji bežični telefon zauzima je gotovo polovica širine Wi-Fi kanala, a snaga emitiranja je dvostruko veća. Ukoliko se koristi model koji radi na 2.4 GHz, preporuča se postaviti ga dalje od Wi-Fi pristupne točke kako ne bi došlo do ometanja. Ipak, najbolji izbor bi bio neki model bežičnog telefona koji radi u drugom frekvencijskom području.

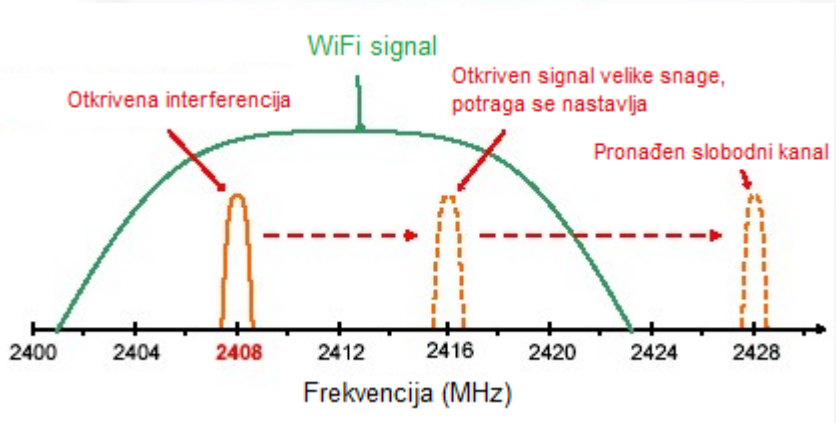


Slika 6. Širine kanala i snage emitiranja u području 2.4 GHz
Izvor: EETimes

Bluetooth uređaji stvaraju proizvoljnu (*ad-hoc*) mrežu malog dometa, a podatke prenose pomoću radiovalova na frekvencijama u ISM pojasu na 2.4 GHz. Širina kanala kojeg koriste Bluetooth uređaji je svega 1 MHz. Dodatno, frekvencijsko područje na 2.4 GHz je podijeljeno na 79 kanala od 1 MHz, a svaki Bluetooth uređaj 1600 puta u sekundi slučajnim odabirom promijeni kanal u

kojem prenosi podatke. Zbog ovakvog načina rada i male širine kanala, Bluetooth ne može uzrokovati velike probleme za WLAN mrežu, ali WLAN mreža može značajno narušiti dostupnost Bluetooth uređaja. Pokazalo se da WLAN mreža uzrokuje interferenciju na 25% Bluetooth kanala zbog čega se paketi moraju ponovo slati što rezultira manjim brzinama prijenosa. Zbog toga je Bluetooth unaprijeđen korištenjem AFH (eng. *adaptive frequency hopping*) algoritma kojim se označavaju koji kanali su dobri (nema interferencije s Wi-Fi signalom), a koji loši (postoji interferencija). Pri promjeni kanala u obzir će se uzimati samo oni kanali koji su označeni kao dobri. Na Bluetooth uređaje također mogu utjecati bežični telefoni, ali vjerojatnost interferencije bežičnog telefona i Bluetooth uređaja je puno manja nego vjerojatnost interferencije bežičnog telefona i Wi-Fi uređaja upravo zbog male širine Bluetooth kanala.

Bežični USB ima sličan način rada kao Bluetooth što se tiče korištenja frekvencijskog spektra. Kao i Bluetooth, koristi 79 kanala širine 1 MHz, ali ih ne mijenja toliko često kao Bluetooth. Bežični USB (eng. *Universal Serial Bus*) koristi pametan algoritam koji mu omogućuje nesmetani suživot s ostalim uređajima u području 2.4 GHz. Prije nego bežični USB odabere kanal u kojem će raditi, provjerava postoje li još neke mreže bežičnog USB-a i koje kanale one koriste. Zatim odabere neki kanal i svakih 50 ms provjerava razinu šuma. Kada ona postane prevelika, traži se novi kanal u kojem je razina šuma prihvatljiva (slika 7). Tako se pronalaze područja između kanala koje koriste Wi-Fi i bežični telefoni. Bluetooth uređaji u svojem skakanju po kanalima mogu naići na kanal kojeg koristi bežični USB, ali se u njemu neće zadržati dovoljno dugo da bežični USB natjeraju na promjenu kanala.



Slika 7. Traženje slobodnog kanala
Izvor: EETimes

ZigBee se koristi za umrežavanje uređaja na malom prostoru koji izmjenjuju malu količinu podataka i zahtijevaju malu potrošnju. ZigBee se koristi u bežičnim prekidačima, senzorskim uređajima, daljinskim upravljačima za garažu i sl. ZigBee koristi 16 unaprijed definiranih kanala širine 3 MHz za svoj rad. Pri slanju podataka koristi sličan mehanizam otkrivanja sudara kao i kod Wi-Fi: prije slanja podatka uređaj osluškuje kanal kako bi minimizirao vjerojatnost pojavljivanja dva paketa u isto vrijeme na istom kanalu. Ukoliko ipak dođe do „sudara“ dva paketa, paketi se ponovo šalju. Zbog toga ZigBee ne mijenja kanal na kojem šalje podatke čak ni kod velikih interferencija. Paketi koje ZigBee uređaj šalje su dovoljno rijetki i mali da ovakav način prijenosa podataka bude uspješan. Ovisno o tome gdje su ZigBee uređaji postavljeni, mogu nakratko ometati Wi-Fi signal (npr. pri otvaranju garaže moguće su interferencije s Wi-Fi signalom ako je pristupna točka blizu prijemnika signala iz daljinskog upravljača). Ipak, prijenos podataka između ZigBee uređaja u pravilu kratko traje pa je stoga i ometanje Wi-Fi signala dovoljno kratko da ga korisnik ni ne primijeti.

3.3. Namjerno ometanje bežičnih mreža

Kod namjernog ometanja bežičnih mreža koriste se posebni odašiljači signala za ometanje, a cilj je izvesti DoS napad, tj. potpuno onemogućiti korištenje bežične mreže. Ometati se mogu sve mreže koje koriste radiovalove, a princip ometanja je u svojoj osnovi uvijek isti: emitirati signal za ometanje na istoj frekvenciji i moduliran na isti način kao signal koji se želi ometati, ali dovoljno

snažan da nadjača napadnuti signal. Najčešće se ometaju signali mobilne telefonije i Wi-Fi mreža.

Na slici 8 prikazan je jedan odašiljač signala za ometanja (eng. *jammer*). Uređaj je relativno malih dimenzija (118 x 62 x 30 mm), a može ometati signale mobilne telefonije i Wi-Fi mreže u krugu od 20 m. Na uređaju se odmah mogu primijetiti četiri antene različitih veličina. Svaka antena odašilje jedan signal za ometanje za određenu frekvenciju. Tri antene se koriste za ometanje signala mobilne telefonije, a jedna ometa Wi-Fi signal. Kao što je objašnjeno u uvodnom poglavlju, mobilni telefoni rade na tri frekvencije zbog čega su potrebne tri antene kako bi se uspješno blokirao signal za mobilne telefone. Za blokiranje Wi-Fi signala dovoljna je jedna antena koja radi na 2.4 GHz budući da je to frekvencija na kojoj radi većina uređaja Wi-Fi standarda (norme 802.11b/g/n).

Frekvencije na kojima radi uređaj na slici 8 su:

- 925 – 960 MHz (GSM),
- 1805 – 1880 MHz (GSM/DCS),
- 2110 – 2170 MHz (3G),
- 2400 – 2483 MHz (Wi-Fi)

Mobilni telefoni rade u *full-duplex* načinu rada što znači da za komunikaciju zapravo koriste dvije različite frekvencije: jednu za odlazni i jednu za dolazni promet. Primjerice, u Republici Hrvatskoj se za 3G mreže (UMTS standard) koriste frekvencije od 2110 do 2170 MHz za dolazi promet (od bazne stanice do uređaja), a frekvencije od 1920 do 1980 MHz za odlazni promet (od uređaja do bazne stanice). Za ometanje signala mobilne telefonije dovoljno je ometati samo jednu od ove dvije frekvencije. Budući da je udaljenost od bazne stanice do odašiljača signala za ometanje veća od udaljenosti između mobilnog uređaja i odašiljača, za ometanje se koristi frekvencija za dolazni promet (u slučaju 3G mreža, radi se o skupu frekvencija oko 2100 MHz). Naime, zbog veće udaljenosti, signal za ometanje ne mora imati veliku snagu da bi nadjačao signal bazne stanice. Zbog ometanja, mobilni uređaj neće moći primati signal bazne stanice pa će zbog toga pokazivati oznaku nedostupne mreže. Većina korisnika neće posumnjati na uređaj za ometanje, nego će zaključiti da se mreža pokvarila ili da se nalaze u području koje nije pokriveno signalom.

Slabiji uređaji za ometanje pokrivaju područje polumjera 9 m, dok snažniji uređaji mogu ometati signal na području polumjera čak 1.6 km. Doseg uređaja za ometanje ovisi o njihovoj snazi, ali i o preprekama u okolini (zidovi, brežuljci, šume itd.).

Slika 8. Uređaj za ometanje bežičnih mreža
Izvor: www.favordeals.com

Različiti signali se mogu koristiti za ometanje, kao što su:

- šum,
- ton,
- puls,
- snimljeni zvukovi.

U nastavku ovog poglavlja će se objasniti navedeni signali.

Kao što je već spomenuto, za uspješno ometanje potrebno je poznavati frekvenciju na kojoj se emitira signal koji se želi ometati i način na koji je moduliran. Na osnovu tih informacija odabire koji signal će se koristiti za ometanje. Taj signal se zatim modulira. Kao i kod svake modulacije, koristi se signal nosioc koji se nalazi na frekvenciji koja se želi ometati. Nakon što se odabere signal nosioc, radi se modulacija, čime je dobiven signal kojeg uređaj za ometanje emitira.

3.3.1. Ometanje pomoću šuma

Kod ovog oblika ometanja signal nosioc se modulira sa signalom koji ima osobine šuma. Koristeći ovaj oblik ometanja povećava se razina šuma na prijemniku zbog čega dolazi do ometanja ispravnog prijema signala. Zbog povećanja šuma, smanjuje se domet odašiljača pa prijemnici moraju biti bliže odašiljaču kako bi primili ispravni signal.

Širina frekvencijskog područja signala za ometanje može biti široka kao cijeli frekvencijski pojas ili toliko uska da zauzima samo jedan kanal ili samo jedan njegov mali dio. Svaki od ovih načina ima svoje prednosti i nedostatke.

Šum koji se koristi je Gaussov šum koji teoretski ima beskonačan spektar što znači da je korištenjem idealnog Gaussovog šuma teoretski moguće cijeli radiofrekvencijski pojas ometati sa šumom. Ako se radi o bijelom Gaussovom šumu, spektar je svugdje jednak što znači da se svi dijelovi radiofrekvencijskog pojasa ometaju jednakom snagom. Obojeni Gaussov šum ima ograničen spektar i češće se koristi jer se s njime može ograničiti djelovanje ometanja na manji dio radiofrekvencijskog spektra. Time se ometa samo određena tehnologija koja koristi taj dio radiofrekvencijskog spektra.

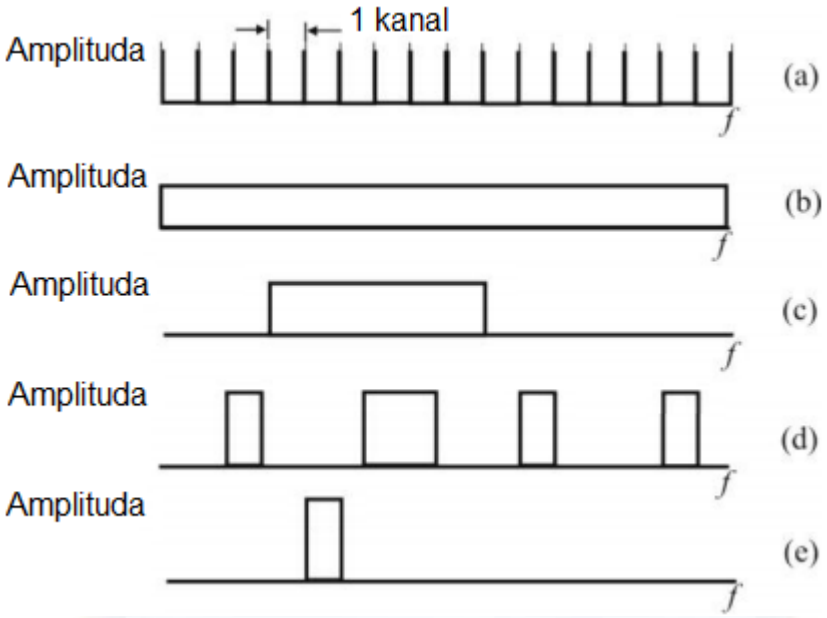
Na slici 9a je prikazan dio radiofrekvencijskog spektra koji je podijeljen na nekoliko kanala. U nastavku će se objasniti utjecaj širine spektra signala šuma na ometanje.

Širokopojasni šum se koristi za ometanje cijelog frekvencijskog pojasa kojeg koristi neka bežična tehnologija (slika 9b). Ovaj tip ometanja djeluje na sve oblike bežičnih mreža. Smanjenjem frekvencijskog područja na kojem se emitira signal za ometanje može se ostvariti veća snaga šuma nego kod emitiranja širokopojasnog šuma što kao posljedicu pruža bolje ometanje (slika 9c). S druge strane, smanjenjem frekvencijskog područja na kojem se emitira šum može doći do ometanja samo manjeg dijela kanala što rezultira slabijim ometanjem.

Šum se može emitirati tako da djelomično pokriva samo neke kanale u frekvencijskom pojasu (slika 9d). Ovakav način ometanja može biti djelotvorniji od širokopojasnog šuma, ako su kanali točno poznati. Na primjer, kod WLAN mreža, za prijenos se može koristiti 13 kanala u frekvencijskom pojasu na 2.4 GHz, ali zapravo se koriste samo tri (kanali 1, 7 i 13). Učinkovitije ometanje se može postići ako se šum emitira samo na ova tri kanala, umjesto na cijeli frekvencijski pojas.

Uskopojasni šum se emitira tako da utječe samo na jedan kanal u frekvencijskom pojasu (slika 9e). Ovaj način ometanja je još učinkovitiji od prethodna dva ako se ispravno primjenjuje, ali zahtjeva poznavanje kanala na kojem se emitira bežični signal. Kod WLAN mreža to ne predstavlja problem, jer svaka pristupna točka koristi samo jedan kanal (kada bi koristila sva tri, moglo bi doći do interferencije s okolnim pristupnim točkama koje također mogu koristiti neki od tri kanala). Ako ometač zna koji kanal WLAN pristupna točka koristi za prijenos podataka, može emitirati takav signal koji koncentrira svu snagu šuma na samo jedan kanal. Ako pristupna točka pokuša promijeniti kanal na kojem radi, može doći do interferencije s okolnim pristupnim točkama koje koriste neki od dva ostala kanala. S druge strane, ako se signal šuma emitira na krivom kanalu, ometanje može biti potpuno neuspješno.

Kod mobilne telefonije, upravljanje kanalima je puno složenije i gotovo je nemoguće točno odrediti koji kanal će koji korisnik koristiti u nekom trenutku.



Slika 9. Prikaz spektra signala za ometanje koji koriste šum
Izvor: Modern Communications Jamming Principles and Techniques

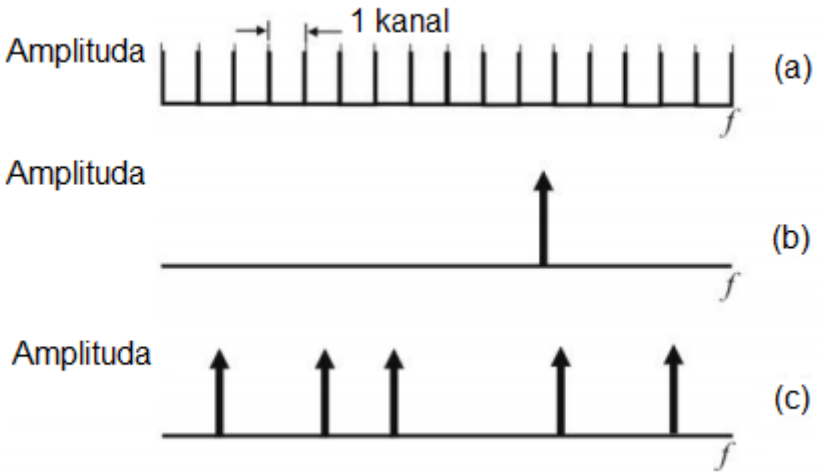
Iz svega navedenog može se zaključiti da je ometanje pomoću šuma jedan od jednostavnijih načina ometanja bežičnih signala. Emitiranje širokopojasnog šuma će sigurno utjecati na kvalitetu bežičnih mreža, a uspješnost ometanja ovisi samo o snazi emitiranog šuma: što je veća snaga emitiranog šuma, manji je SNR pa su i kvaliteta i brzina prijenosa bežičnom mrežom manje. Dovoljno jaki šum može potpuno nadjačati bežični signal i tako izvesti DoS napad. Smanjivanjem širine emitiranog šuma, smanjuje se potrebna snaga emitiranog šuma s kojom se postiže DoS napad, ali je zato potrebno poznavati više informacija o odašiljačima napadnute bežične mreže.

3.3.2. Ometanje pomoću tona

Kod ometanja pomoću tona, jedan ili više tonova se emitira na točno određenim frekvencijama (slika 10). Utjecaj ometanja ovisi o njihovom broju i mjestu gdje su postavljeni. Na slici 10b je prikazan spektar signala za ometanje koji se sastoji od samo jednog tona. Na slici 10c signal za ometanje se sastoji od pet različitih tonova.

Ometanje pomoću jednog tona nije uspješno ako se ometa signal koji koristi tehniku proširenog spektra FHSS (detaljnije objašnjena u poglavlju 4.1). Ovom tehnikom se frekvencija kanala na kojem se emitiraju signali često mijenja pa jedan ton nije dovoljan da ometa cijeli signal. Ometanje će biti uspješno samo kada se signal emitira u blizini frekvencije tona za ometanje. Nešto bolji uspjeh ima ako ometa signale koji koriste DSSS tehniku proširenog spektra (također objašnjena u poglavlju 4.1).

Više tonova u signalu za ometanje koji su pravilno postavljeni mogu uzrokovati puno veće ometanje od samo jednog tona, ali je potrebna snaga signala za ometanje nešto veća. Ako je način odabira kanala za bežični prijenos poznat, tonovi se mogu tako postaviti da potpuno onemoguće komunikaciju bežičnom mrežom.



Slika 10. Prikaz spektra signala za ometanje koji koriste ton
Izvor: Modern Communications Jamming Principles and Techniques

3.3.3. Ometanje pomoću pulsa

Kod ometanja pomoću pulseva signal za emitiranje se oblikuje kao niz, najčešće periodičkih, kratkih pulseva. Kratki pulsevi imaju spektar sličan širokopojasnom šumu, a njihov utjecaj je sličan kao kada se koristi šum koji utječe na samo neke kanale (slika 9d). Prednost u odnosu na prethodno opisane metode ometanja je što zahtjeva manju snagu kako bi proizveo isti ili čak i bolji učinak. Posljedice ometanja ovise o snazi emitiranih pulseva i brzini emitiranja. Ometanje pomoću pulseva je jako učinkovito protiv tehnika proširenog spektra (objašnjene u poglavlju 4.1).

3.3.4. Ometanje pomoću zvukova

Ovaj način ometanja umjesto šuma, tonova i pulseva koristi snimljene glasove, zvukove ili glazbu koju modulira na željenu frekvenciju, pojačava i zatim odašilje. Uređaj za ometanje je relativno jednostavno napraviti, ali uspješnost ometanja može jako varirati i u pravilu je lošija od prethodno opisanih metoda. Ipak, uz dovoljno jaku snagu signala za ometanje, može se izvesti DoS napad.

4. Zaštita od ometanja

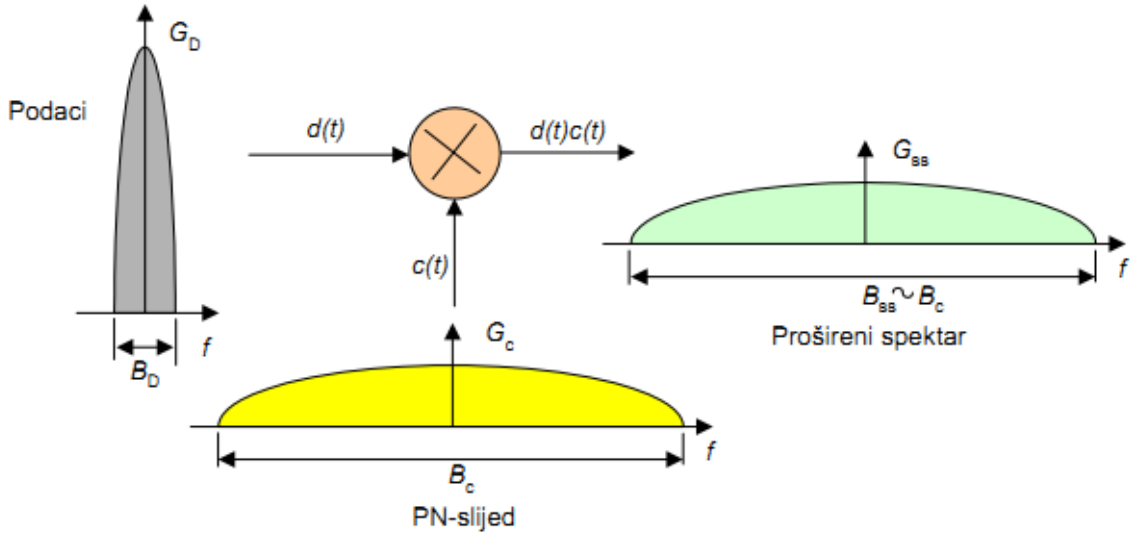
Zbog čestog korištenja ometanja bežičnih mreža razvijene su neke tehnike zaštite od takvog oblika napada. Te tehnike su danas uključene u standarde bežičnih mreža, ali unatoč njima, s dovoljno jakim signalom za ometanje i najbolja zaštita od ometanja može se pokazati nedovoljnom. Na sreću, uređaji za ometanje koji emitiraju signale s velikom snagom ne mogu dugo raditi.

4.1. Tehnike proširenog spektra

Najpoznatiji oblik zaštite od ometanja je korištenje tehnika proširenog spektra. To su tehnike DSSS i FHSS.(

Kod DSSS tehnike signal *d(t)* (modulirani signal koji se inače emitira) se prije emitiranja množi s nizom impulsa *c(t)* koji su dio PN (eng. *Pseudorandom Numerical*) slijeda kao na slici 11. PN slijed bi trebao imati osobine šuma i njegov spektar bi trebao biti puno širi od početnog signala *d(t)*. Nakon množenja ova dva signala, spektar dobivenog signala je otprilike jednako širok kao spektar signala *c(t)*. Izvorni signal je 'sakriven' u šumu i za sve prijemnike koji ne znaju da se radi

o DSSS signalu on predstavlja širokopojasni šum male snage. Na prijemnoj strani DSSS signal se ponovo množi s istim PN slijedom, a zatim filtrira na širinu izvornog signala *d(t)* kako bi se dobio izvorni signal.



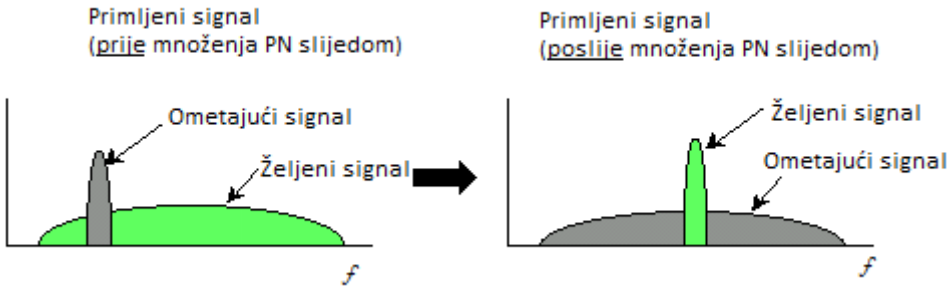
Slika 11. Dobivanje DSSS signala
Izvor: zrk.fer.hr

DSSS može jednostavno ukloniti neželjene signale, uključujući signale za ometanje. Ključne stvari koje treba primijetiti kod DSSS tehnike su sljedeće:

1. Množenje PN slijedom **jednom** širi frekvencijski pojas signala.
2. Množenje PN slijedom **dvaput**, uz filtriranje, dovodi do izvornog signala.
3. Željeni signal se množi **dvaput**, a ometajući signal samo **jednom**!

Sada je jasno zašto DSSS tehnika može spriječiti ometanje. Na prijemnu stranu će doći DSSS signal zajedno sa signalom za ometanje, ali množenjem s PN slijedom u prijemniku, DSSS signal će se skupiti, a ometajući signal raširiti u spektru (slika 12). Filtriranjem će samo manji dio signala za ometanje proći dalje što znači da signal za ometanje neće jako utjecati na izvorni signal.

Nedostatak DSSS tehnike je što emitira signal male snage što znači da signal za ometanje ne mora biti jako snažan da nadjača DSSS signal. Širokopojasni šum jače snage od DSSS signala može vrlo lako izvesti DoS napad.



Slika 12. Obrada DSSS signala na prijemnoj strani
Izvor: www.wireless-telecom.com

FHSS tehnika također koristi PN slijed, ali u druge svrhe. Kod FHSS tehnike frekvencija nosioca signala se stalno mijenja, a odabir frekvencije ovisi o PN slijedu. To znači da će se signal svaki

puta prenositi na nešto drugačijoj frekvenciji, ali naravno, uvijek u dodijeljenom frekvencijskom pojasu. Prijemnik mora znati PN slijed kako bi znao gdje se u frekvencijskom području nalazi signal. Dodatno, odašiljač i prijemnik moraju biti jako dobro sinkronizirani.

Ova tehnika širokog spektra je jako učinkovita protiv ometanja koji je ograničen na samo neke kanale, a ne na cijeli frekvencijski pojas. Naime, ako ometač ne zna PN slijed, ne može znati u kojem dijelu frekvencijskog pojasa se nalazi signal kojeg bi trebao ometati. Ako ga i uspije pronaći, signal će se ubrzo preseliti na neko drugo frekvencijsko područje i tako izbjeći ometanje. Ipak, ako se koristi širokopojasni šum za ometanje, onda FHSS nije toliko učinkovit kao DSSS jer i manje snage šuma mogu ometati FHSS signal više nego što ometaju DSSS signal. Kada je signal širokopojasnog šuma dovoljno snažan, ni FHSS ni DSSS neće puno pomoći kod ometanja.

Ometanje pomoću tonova daje bolje rezultate od ometanja šumom kada se radi o signalu koji koristi prošireni spektar. Već i ometanje sa samo jednim tonom može nadjačati DSSS signal, ako ton titra pravom frekvencijom i dovoljnom snagom. Ako uređaj za ometanje ima ograničenu snagu emitiranja, onda se bolji rezultati postižu s više tonova u signalu za ometanje.

4.2. Zaštita na razini bitova

Iako tehnike proširenog spektra mogu pružiti dosta dobru zaštitu, sve bežične mreže imaju dodatnu zaštitu na razini bitova. Čak i ako ometanje nije dovoljno snažno da se izvede DoS napad i potpuno onemogući razmjena paketa radiovalovima, signal za ometanje može „oštetiti“ pakete na njihovom putu. Već jedan krivi bit može izazvati velike greške prilikom dekodiranja primljenih podataka ili uzrokovati odbacivanje cijelog paketa. Zbog toga se koriste metode zaštite bitova.

Tehnike koje se koriste dodaju redundantne bitove u pakete koji ne nose korisne informacije, ali pomažu u ispravljanju krivih bitova. Postupak se zove FEC (eng. *Forward error correction*), a pomaže i kod prirodnih interferencija radiovalova.

Konvolucijski koderi su jedna od tehnika koja se koristi kod FEC postupka, a pomaže u ispravljanju slučajnih pogrešaka. Druga često korištena tehnika je Reed-Solomon postupak kojim je moguće otkloniti greške u uzastopnim bitovima. Ovi koderi dodaju nekoliko dodatnih bitova, a što se više redundantnih bitova doda, to će se više grešaka pri prijenosu moći ispraviti. Najčešće se navodi koliki je omjer redundantnih bitova i svih bitova koji se prenose. Omjer od 1:2 je najrobusniji, ali s druge strane znači da pola prenesenih bitova ne nosi korisničke informacije i zapravo se brzina prijenosa korisnih podataka smanjuje. Omjer se kod boljih sustava dinamički mijenja, ovisno o stanju prijenosnog kanala. Ako su smetnje snažne, koristit će se veći broj zaštitnih bitova u kombinaciji s nekom robusnijom modulacijskom metodom poput BPSK. Brzina prijenosa će svakako biti manja, ali smanjit će se potreba za ponovnim slanjem paketa koji su odbačeni zbog prevelikog broja krivih bitova koje nije moguće ispraviti. Kada se stanje u kanalu popravi, bitovi se mogu štititi s manje redundantnih bitova kako bi se omogućile veće brzine prijenosa korisnik podataka.

Jedna od često korištenih tehnika kojom se smanjuju posljedice krivo primljenih bitova je raspršivanje podataka. Kod ove tehnike bitovi se ne odašilju onim redoslijedom kojim su nastali, nego se međusobno izmiješaju prije slanja. Ukoliko dođe do greške pri prijenosu najčešće dođe do promjene nekoliko uzastopnih bitova. Ako se bitovi prije odašiljanja rasprše, greška pri prijenosu u nekoliko uzastopnih bitova će se također rasprštiti. Tako se mogu bolje iskoristiti konvolucijski koderi koji su nemoćni ako je nekoliko uzastopnih bitova pogrešno.

5. Zaključak

Bežične mreže su puno ranjivije na napade od žičanih mreža. Jedan od čestih oblika napada na bežične mreže je ometanje signala ili *jamming* s ciljem izvođenja DoS napada. Za ometanje potrebno je poznavati tri stvari o signalu kojeg se želi ometati: frekvenciju na kojoj se emitira, modulacijsku tehniku koju koristi i njegovu snagu. Ovisno o signalu kojeg se želi ometati, odabire se neki signal za ometanje, modulira na isti način i na istu frekvenciju kao i ciljani signal i emitira snagom većom od napadnutog signala. U svojoj osnovi je ometanje signala vrlo jednostavno. S dovoljno jakim signalom, primjerice šuma, moguće je ometati gotovo sve bežične mreže.

Ipak, problem je napraviti uređaj za ometanje koji će jako dugo i na velikom području emitirati dovoljno jaki signal za ometanje. Naravno, moguće ga je napraviti, ali krajnja cijena može biti toliko velika da nije isplativo raditi takav uređaj. Zbog toga se koriste neke pametnije tehnike za ometanje. Uz malo više informacija o signalu kojeg se želi ometati, s istom snagom emitiranog signala za ometanje, mogu se napraviti puno veće štete.

Tehnike koje bi trebale štititi od ometanja signala postoje, ali one su manje razvijene od tehnika za ometanje. Problem je što tehnike protiv ometanja signala ili anti-jamming tehnike korisnik ne može samo „ugraditi“ u svoj uređaj koji koristi za pristup bežičnoj mreži. Ne postoji zakrpa koja unaprjeđuje WiFi antenu u prijenosnom uređaju pa da on bude otporniji na smetnje. Tehnike protiv ometanja signala mora ugraditi proizvođač, a to se ne može napraviti dok anti-jamming tehnika ne postane dio standarda za uređaje određene bežične tehnologije. Može se zaključiti da su „napadači“ u određenoj prednosti.

Za kraj, treba imati na umu da nisu sva ometanja bežičnog signala namjerna. Kada dođe do pada kvalitete prijema bežičnog signala ne treba odmah zaključiti da se radi o napadu ometanjem. Najvjerojatnije je došlo do problema pri prijenosu bežičnog signala zbog određenih atmosferskih uvjeta ili raspored okolnih objekata nepovoljno utječe na širenje radiovalova. Postoji mogućnost da se negdje u blizini koristi uređaj koji radi na istoj frekvenciji kao ometani uređaj pa dolazi do interferencije. Ovi slučajevi su vrlo česti kada se radi o bežičnim tehnologijama koje rade u besplatnom frekvencijskom pojasu na 2.4 GHz.

6. Leksikon pojmova

DOS napad (Napad uskraćivanjem usluge)

Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad.

http://searchsoftwarequality.techtarget.com/definition/denial-of-service

Bežična pristupna točka (Uređaj koji korisniku omogućuje bežični pristup računalnoj mreži)

Bežična pristupna točka (eng. *Wireless access point*) je uređaj koji omogućuje bežičnim korisnicima (uređajima) pristup računalnoj mreži pomoću Wi-Fi, Bluetooth ili sličnih standarda. WAP se obično spaja na usmjerivač i može prenositi podatke između bežičnih uređaja i žičanih uređaja na mreži.

http://compnetworking.about.com/cs/wireless/g/bldef_ap.htm

3G (Tehnologija treće generacije mobilne telefonije)

Nadogradnja SIM/USIM tehnologije, omogućuje brži prijenos podataka bežičnim putem. 3G mreže nude nove usluge kao što su prijenos pokretnih slika, pristup globalnoj mreži Internet, mobilna televizija i video pozivi. Dodatno, omogućuje autentifikaciju mreže, što prije nije bilo moguće.

http://searchtelecom.techtarget.com/definition/3G

UMTS (Universal Mobile Telecommunications System)

UMTS je treća generacija tehnologije mobilnih telefona za mreže temeljene na GSM standardu. UMTS koristi W-CDMA tehnologiju u pristupnoj mreži kako bi ostvarila bolju spektralnu učinkovitost. UMTS pokriva cijelu mobilnu mrežu: pristupnu mrežu (UTRAN), jezgrenu mrežu i autentikaciju korisnika pomoću SIM kartica.

http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

WiMax (Worldwide Interoperability for Microwave Access)

WiMax je bežična mreža za širokopojasni pristup Internetu za fiksne ili mobilne korisnike. Trenutačna inačica WiMax standarda omogućuje brzine do 40 Mbit/s. Predstavlja alternativu mobilnim mrežama jer pruža veće brzine.

http://info.biz.hr/Typo3/typo3_01/dummy-3.8.0//index.php?id=485

7. Reference

[1] Ryan Winfield Woodings, Mark Gerrior: Avoiding Interference in the 2.4-GHz ISM Band, http://www.eetimes.com/design/microwave-rf-design/4012556/Avoiding-Interference-in-the-2-4-GHz-ISM-Band?pageNumber=1, siječanj 2006.

[2] Wikipedia: Radio jamming, http://en.wikipedia.org/wiki/Radio_jamming, kolovoz 2011.

[3] Richard Poisel: Modern Communications Jamming Principles and Techniques, Second Edition, 2011.

[4] Gary Wollenhaupt: How Cell Phone Jammers Work, http://electronics.howstuffworks.com/cell-phone-jammer.htm, ožujak 2005.

[5] Krešimir Malarić: Zaštita radiokomunikacijskih sustava, 2005.