Sustavi za praćenje i vođenje procesa

Branko Jeren i Predrag Pale
Fakultet elektrotehnike i računarstva
Zavod za elektroničke sustave i obradbu signala

Bežične mreže
Wireless Ethernet

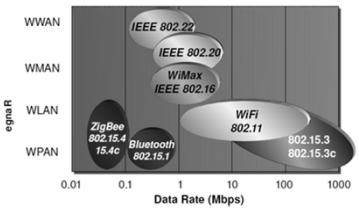
Pregled

- standard
- tehnologija bežične komunikacije
- frekvencije
  - ISM
  - *spread spectrum*
  - modulacije
- konfiguracija mreža
  - *point-to-point*
  - ad-hoc
  - infrastrukturne
  - Ap i načini rada
- protokol
- domet
  - kabeli
  - antene
  - smetnje

- prednosti
- nedostaci
- sigurnost

Standard(i)

- danas postoji mnoštvo tehnologija i standarda
- najčešće mislimo na "obitelj" IEEE 802.11
  - njih često zovu i WiFi
  - iako nije strogo definirano na koji standard se odnosi
- još postoje
  - infracrvene mreže
  - Bluetooth
  - ZigBee
  - WiMax
  - ...



IEEE 802.11

Standardi	**802.11b**	**802.11a**	**802.11g**	**802.11n**
Maksimalna brzina [Mbps]	11	54	54	600
Stvarna brzina [Mbps]; 3m	6	25	25	
Stvarna brzina [Mbps]; 30m	6	12	20	
Frekvencija [GHz]	2.4	5	2.4	2.4 ili 5
Modulacija	DSSS, CCK	OFDM	DSSS, CCK, OFDM	DSSS, CCK, OFDM+
Širina kanala [MHz]	20	20	20	20 ili 40

Ovi su standardi rasprostranjeni u praksi

Standardi u razvoju

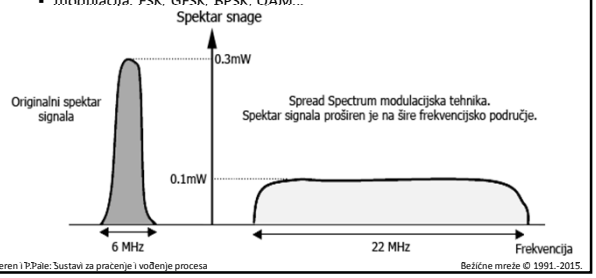
- 802.11-2012 (802.11mb)
  - update i „čišćenje" 802.11n
- 802.11ac
  - dogradnja 802.11n
  - kanali 80 ili 160 MHz
    - (umjesto 40)
  - do 8 paralelnih streamova
    - (umjesto 4)
  - 5GHz
  - modulacija 256 QAM
    - (umjesto 64 QAM)
  - trenutno (od 2013.) 1300Mbps
    - 80MHz/3stream/256QAM = 433.3*3
- 802-11ad – 7 Gbps
  - 60GHZ band
  - WiFI Alliance
- 802-11af
  - White-Fi – TV band 54-790 MHz
  - OFDM based on 802-11ac
- 802-11ah – ožujak 2016.?
  - sub 1GHz nelic. band
  - bolja propagacija
  - velike senzorske mreže

Frekvencije: ISM opseg

- *Industrial, Scientific* & *Medical*
- tri opsega
  - 902 – 928 MHz
  - 2.4 – 2.4835 GHz
  - 5.728 – 5.750 GHz
- "nelicenciran"
  - ne treba dozvola za korištenje
  - na svjetskoj razini
    - i u Hrvatskoj
  - i **ne plaća se** korištenje
- svaka zemlja ipak propisuje
  - točnu frekvenciju
  - broj korištenih kanala
  - max izlaznu snagu
- u Hrvatskoj
  - koristi se 13 kanala, po 5 MHz
  - 100 mW
  - usporedba
    - GSM je max. dozvoljeno 2 W !!!

Frekvencije: *Spread Spectrum*

- 50-tih godina 20. stoljeća
- prva koristila američka vojska
- skrivanje signala unutar šuma u komunikacijskom kanalu
  - PN (eng. *pseudo noise*) signal valnog oblika poput šuma
  - PN * informacija => proširuje osnovni spektar snage signala na šire frekvencijsko područje
  - modulacija: FSK, GFSK, BPSK, QAM...

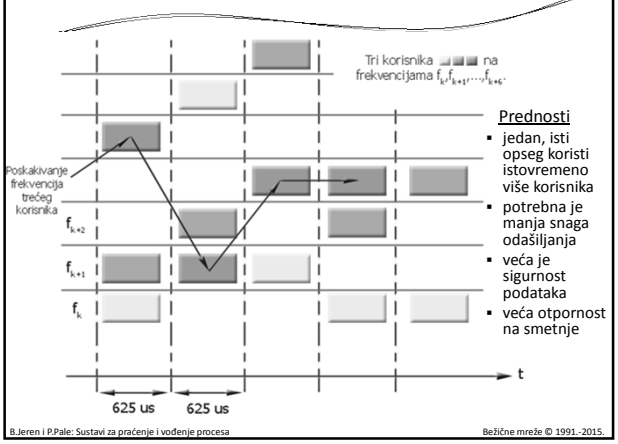


Frekvencije: *Spread Spectrum*

- *Spread Spectrum* se može realizirati jednom od tehnika:
  - FHSS
  - DSSS
  - DS/FHSS: hibrid FHSS i DSSS tehnike

Frekvencije: FHSS tehnika

- FHSS tehnika (eng. *Frequency Hopping Spread Spectrum)*
- cijeli se frekvencijski opseg (ISM) podijeli na 79 kanala širine 1MHz
- tijekom emitiranja mijenja frekvencije ("skače") po unaprijed određenom i dogovorenom slijedu
  - do 1600 puta u sekundi
  - emitiranje informacije na istom kanalu („ *time slot") = 625μs*
- ako nastane greška
  - emitira se ponovno, na drugom kanalu
- i odašiljač i prijemnik su upoznati sa slijedom preskakivanja radi neprekinutog održavanja veze
- koristi GFSK modulaciju signala
  - *Gaussian Frequency Shift Keying*

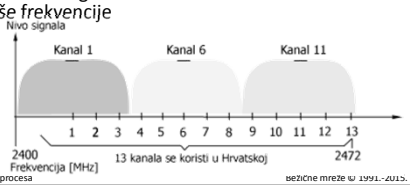


Prednosti

- jedan, isti opseg koristi istovremeno više korisnika
- potrebna je manja snaga odašiljanja
- veća je sigurnost podataka
- veća otpornost na smetnje

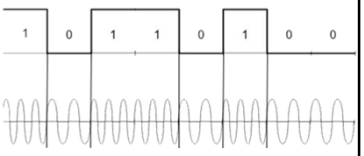
Frekvencije: DSSS tehnika

- DSSS tehnika (eng. *Direct Sequence Spread Spectrum)*
  - ili DS-CDMA (*Direct Sequence code division multiple access)*
- frekvencijski opseg (ISM)
  - dijeli se na 13 kanala (Hrvatska)
    - razmaknuti 25MHz
    - kanali se ne preklapaju
  - uzima se svaki 5. kanal
    - jer podatke množimo PN signalom (pseudo noise) više frekvencije
      - 01001000111
  - istovremeno do 3 korisnika(max)
  - može koristiti modulacije signala
    - FSK, GFSK, BPSK

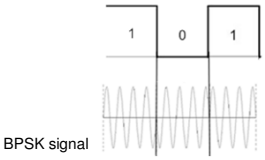


Frekvencije: Modulacije

- modulacije signala za FHSS i DSSS tehnike
  - FSK (*Frequency Shift Keying)*



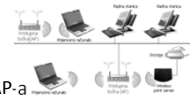
  - GFSK = *Gaussian* filtar + FSK (*Gaussian Frequency Shift Keying)*
  - BPSK (*Binary Phase Shift Keying)*



Konfiguracija mreža

- računala se mogu spajati na dva osnovna načina
  - **ad-hoc** mreže

    - dva (eng. *point-to-point*) ili više računala
    - bez središnje pristupne točke *(*eng. *access point = AP)*
    - sva računala moraju biti međusobno u dometu radio signala
  - **infrastrukturne** mreže

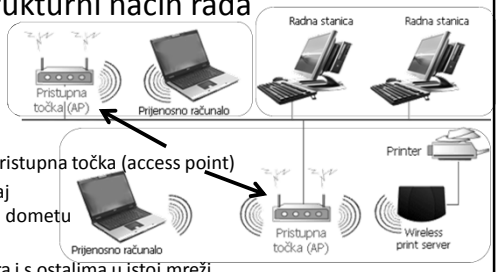


    - koristi se središnja pristupna točka
    - svaki uređaj mora biti u dometu samo AP-a
    - moguće je slagati složene infrastrukture
      - s više AP-ova

Ad-hoc način rada

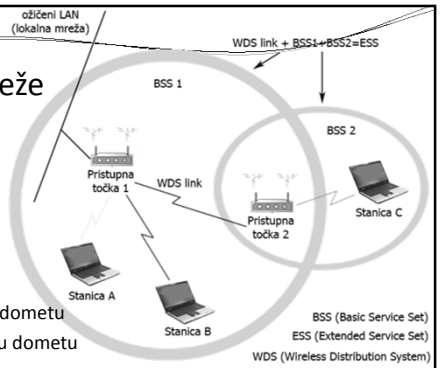
- dva (eng. *point-to-point*) ili više računala
- bez središnje pristupne točke AP (eng. *access point*)
- sve stanice moraju biti međusobno u dometu radio signala

Infrastrukturni način rada



- koristi se pristupna točka (access point)
- svaki uređaj mora biti u dometu samo AP-a
  - ne mora i s ostalima u istoj mreži
  - s njima komunicira posredstvom AP-a
- moguće je slagati složene infrastrukture
  - s više AP-ova

Složene mreže



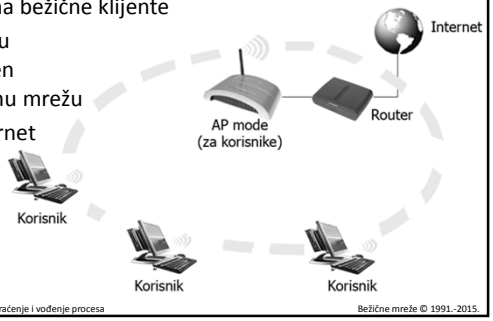
- više AP-ova
  - međusobno u dometu
- korisnik mora biti u dometu
  - samo svog AP-a
- vezu sa "žičanom mrežom"
  - dovoljno je da ima samo jedan AP

AP – *Access Point*

- „pristupna točka" tj. uređaj
  - za povezivanje uređaja u bežičnu mrežu – infrastrukturni WLAN
- radi na 4 načina
  - AP ***root*** *mode*
  - AP ***client*** *mode*
  - AP ***repeater*** *mode*
  - AP ***bridge*** *mode*

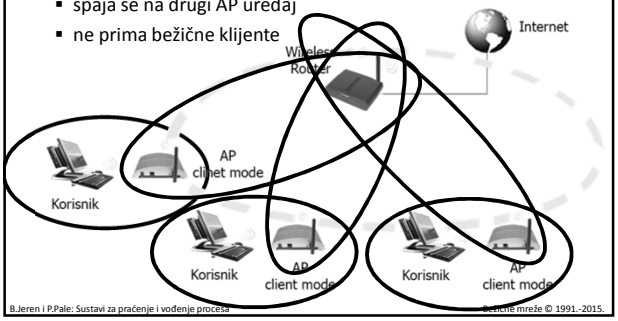
AP ***root*** *mode*

- AP radi kao središnja pristupna točka
  - prima bežične klijente
- u pravilu je spojen na žičanu mrežu
  - Internet



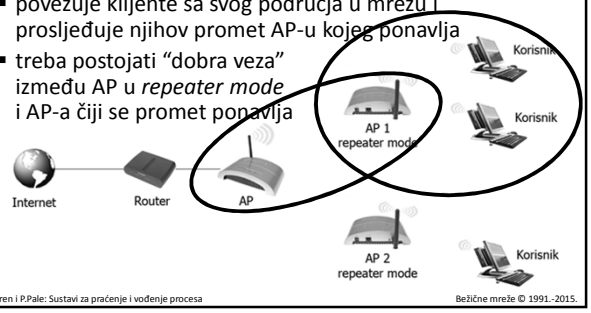
AP ***client*** *mode*

- AP se ponaša kao klijent "glumi" bežičnu mrežnu karticu
  - spaja se na drugi AP uređaj
  - ne prima bežične klijente



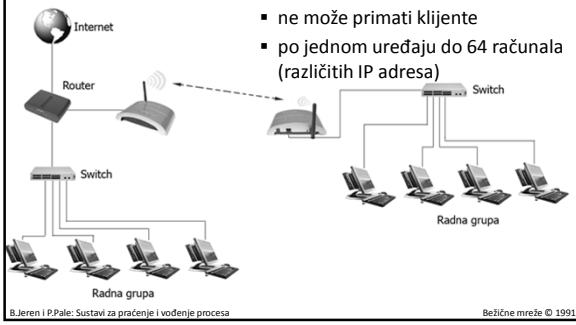
AP ***repeater*** *mode*

- AP radi kao *repeater*
- ponavlja signal drugog AP
- povezuje klijente sa svog područja u mrežu i prosljeđuje njihov promet AP-u kojeg ponavlja
- treba postojati "dobra veza" između AP u *repeater mode* i AP-a čiji se promet ponavlja



AP ***bridge*** *mode*

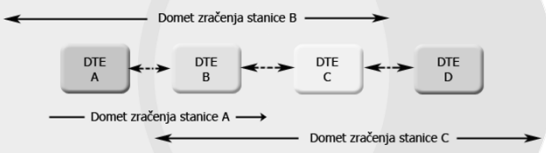
- AP radi kao *bridge*
  - spaja dvije (eng. *point-to-point*) ili više mreža (eng. *point-to-multipoint*)
  - ne može primati klijente
  - po jednom uređaju do 64 računala (različitih IP adresa)



Protokol

- centralizirani ili decentralizirani višestruki pristup mediju
- CSMA/CA protokol
  eng. *Carrier Sense Multiple Access with Collision Avoidance*
  - višestruki pristup mediju s izbjegavanjem sudara okvira
- **Decentralizirani** pristup mediju
  - **izravna komunikacija** između čvorova
  - problem **skrivene** stanice (eng. *hidden station problem*)
  - problem **izložene** stanice (eng. *exposed station problem*)
- **Centralizirani** pristup mediju
  - **ne postoji izravna** komunikacija između čvorova, već preko AP-a

Problem skrivene i izložene stanice



- Problem **skrivene** stanice
  - A šalje prema B-u
  - A nije u dometu C
  - pa C „misli" da može istovremeno slati B-u
  - B prima oba paketa istovremeno i nastaje kolizija

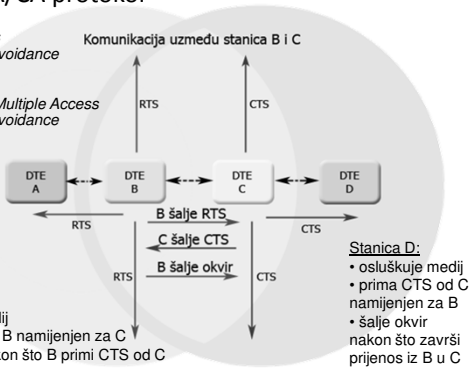
Postaje jasno da CSMA/CD **nije primjeren** bežičnoj okolini

- Problem **izložene** stanice
  - B šalje prema A-u
  - C je u dometu B pa C „misli" da ne može istovremeno slati D-u
  - No, kad i bi slao B bi uočio koliziju i odustao od slanja prema A-u

CSMA/CA protokol

MACA
Multiple Access with Collision Avoidance

CSMA/CA
Carrier Sense Multiple Access with Collision Avoidance

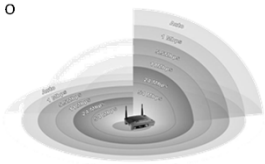


Stanica A:
- osluškuje medij
- prima RTS od B namijenjen za C
- šalje okvir nakon što B primi CTS od C

Stanica D:
- osluškuje medij
- prima CTS od C namijenjen za B
- šalje okvir nakon što završi prijenos iz B u C

Domet

- **ne može se predvidjeti**, jer ovisi o
  - preprekama
  - smetnjama
  - antenama
  - intenzitetu korištenja



- može se računati na:
  - i **do 100 m** u prostoru **bez zidova**
  - oko **20 m u zgradama**, kroz zidove
    - pa i manje ako je puno metala i debelih armiranih zidova
  - više stotina metara na otvorenom
  - nekoliko km s usmjerenim antenama
- ali propusnost se uopće ne može predvidjeti
  - i mijenjat će se s vanjskim okolnostima

Prednosti i nedostaci

- Prednosti
  - **lagano se uspostavlja**
    - idealan za privremene mreže
  - **jeftino**
  - može se koristiti i za **povezivanje dvije fiksne** mreže
    - udaljene lokacije
    - na veću udaljenost usmjerenim antenama

- Nedostaci
  - dijeljeni medij
    - svi se korisnici natječu za prijenos podataka -> **manja propusnost**
  - prenapučenost spektra
    - **smetnje** od drugih korisnika
  - teško se ograničava samo na željeno područje
    - **ometa** druge
    - **lagano se prisluškuje**
  - u istom opsegu rade i industrijski uređaji
    - mikrovalna pećnica, …

Sigurnost komunikacije i podataka

- napadi
  - neovlašteno korištenje mreže
  - prisluškivanje
  - lažni korisnici – "*Man in the middle*" napad
  - lažni AP
- obrana kriptiranjem prometa
  - WEP nije dovoljno siguran
  - WPA i WPA2 – dovoljno sigurni
  - šifre
    - unaprijed dogovorena (eng. *pre shared key*)
    - puno bolje je autentikacijski server -> RADIUS
- osim toga može se
  - skrivati SSID mreže
  - filtrirati prema MAC adresi
  - smanjiti izlazna snaga, antene usmjeriti na unutrašnjost objekta
- unatoč tome, zlonamjerni mogu
  - preopteretiti servise - "*Denial of service*" napad
  - ometati radijski spektar

Napadi na sigurnost

- neovlašteno korištenje mreže
- prisluškivanje
- lažni korisnici
- presretanje veze – "*Man in the middle*" napad
- lažni AP

- *Denial of Service*
- ometanje radijskog spektra

Neovlašteno korištenje mreža

- priključivanje na nečiju bežičnu mrežu
- najčešće u svrhu pristupa globalnom Internetu
- aktivno korištenje
  - može se otkriti

Prisluškivanje

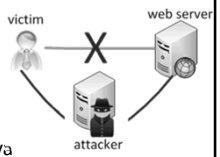
- pasivno korištenje
  - pa se ne može otkriti
- moguće je zato što se elektromagnetski valovi šire i izvan željenog područja
- napadaču je dostupno sve
  - i protokol
  - i identifikacije
  - i adrese
  - i sadržaj komunikacije
- često je i predradnja za druge napade
  - čak i kod kriptirane komunikacije

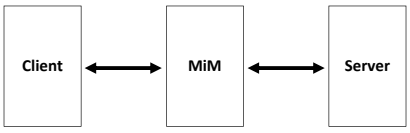
Lažni korisnici

- lažno predstavljanje kao legitimni korisnik
- prethodno je potrebno prisluškivati
  - otkriti legitimne korisnike
    - MAC adresu
    - autentikacijske podatke
- dvije metode
  - ili čekati da legitimni korisnik prestane s radom
  - ili istovremeno
    - napadati legitimnog korisnika
      - deauthentication, dissassociation
    - predstavljati se u njegovo ime
- čak i kad se otkrije lažno predstavljanje
  - ne znamo gdje je napadač

Presretanje veze

- "Man in the middle" napad
  - injection - ubacivanje podataka
  - key manipulation – promjena ključeva
  - downgrade attack – forsiranje starijih protokola
  - filtering





Presretanje veze – injection

- legitimni korisnik uspostavi vezu (autentikacija, …)
- a napadač pored legitimnih podataka za i od klijenta
- dodaje svoje
  - naredbe
  - davanje lažnih odgovora (servera) klijentu
- posebno važno
  kad je veza zaštićena jednokratnom zaporkom

Presretanje veze – key manipulation

- ključeve koji se koriste za druge sustave zaštite
  - SSH, IPSEC, HTTPS
- može se lažirati ključeve

Presretanje veze – downgrade attack

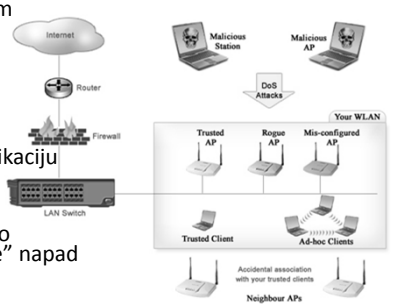
- ubacivanje parametara
  - u razmijenjene podatke između klijenta i servera
- koji forsiraju korištenje starijih protokola
- koji imaju slabosti
  - i mogu se zaobići
  - ili zloupotrijebiti

Presretanje veze – filtering

- legitimnom korisniku se propuštaju samo neki dolazni i/ili odlazni podaci
- ugrađivanje zlonamjernog koda u web stranice
- ugrađivanje virusa u datoteke koje se downloadaju

Lažni IP

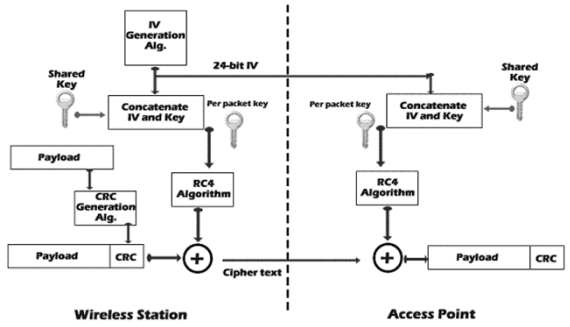
- onesposobi se legitimni AP
  - npr. DoS napadom
- aktivira se lažni AP
  - koji preuzme sve veze i komunikaciju
- dalje funkcionira kao "Man in The Middle" napad



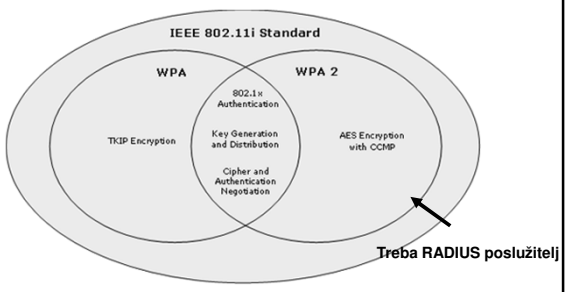
Osnovna obrana – kriptiranjem prometa

- WEP **nije dovoljno siguran**
- WPA i WPA2 – dovoljno sigurni
- šifre
  - **unaprijed dogovorena** (eng. *pre shared key*)
  - puno bolje je koristiti neki autentikacijski server
    - npr. RADIUS

WEP protokol – inicijalizacija veze



WPA vs. WPA2

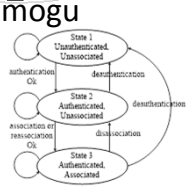


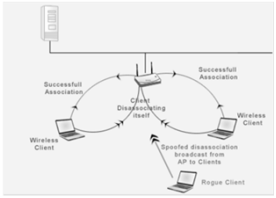
Dodatne metode obrane

- **skrivati SSID** mreže
- **filtrirati** prema **MAC** adresi
- **smanjiti** prodiranje **signala** izvan željenog područja
  - **smanjiti** izlaznu **snagu**
  - **antene usmjeriti** na unutrašnjost objekta

Unatoč tome, zlonamjerni mogu

- preopteretiti servise
  "*Denial of service*" napadi
  - "*disassociation attack*"
    - napad na klijenta
    - napadač glumi AP i naređuje klijentu da se odspoji
    - klijent će ponovo pokušati uspostaviti spoj
    - ali ako dobiva veliku količinu "*disassoc*" paketa, bit će zapravo blokiran
  - "*dautehntication attack*"
    - svi klijenti gube komunikaciju „ispadaju iz mreže"
  - "*authentication attack*"
    - preplaviti AP "*deauth*" paketima
  - i još ...
    - Time window attack
    - Virtual carrier sense attack
  - ometati radijski spektar

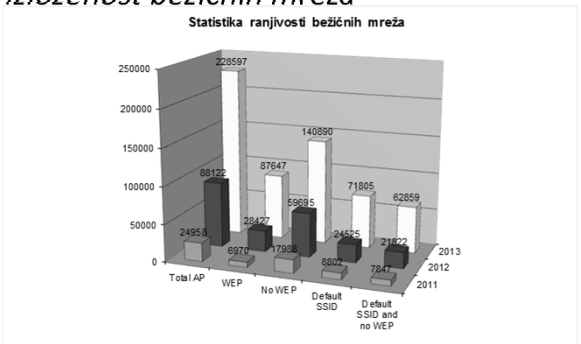




Sigurnost komunikacije i podataka

- napadi
  - neovlašteno korištenje mreže
  - prisluškivanje
  - lažni korisnici – "*Man in the middle*" napad
  - lažni AP
- obrana kriptiranjem prometa
  - WEP nije dovoljno siguran
  - WPA i WPA2 – dovoljno sigurni
  - šifre
    - unaprijed dogovorena (eng. *pre shared key*)
    - puno bolje je autentikacijski server -> RADIUS
- osim toga može se
  - skrivati SSID mreže
  - filtrirati prema MAC adresi
  - smanjiti izlazna snaga, antene usmjeriti na unutrašnjost objekta
- unatoč tome, zlonamjerni mogu
  - preopteretiti servise - "*Denial of service*" napad
  - ometati radijski spektar

Izloženost bežičnih mreža



Predrag.Pale@FER.hr
SPVP.zesoi.fer.hr

