

# Sustavi za praćenje i vođenje procesa

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

---

---

---

---

---

---

---

---

# 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

---

---

---

---

---

---

---

---

## Frekvencije: ISM opseg

- *Industrial, Scientific & Medical*
- tri opsega
  - 902 – 928 MHz
  - 2.4 – 2.4835 GHz
  - 5.728 – 5.750 GHz
- "nelicenciran", tj. 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 (za GSM je max. dozvoljeno 2 W !!!)

---

---

---

---

---

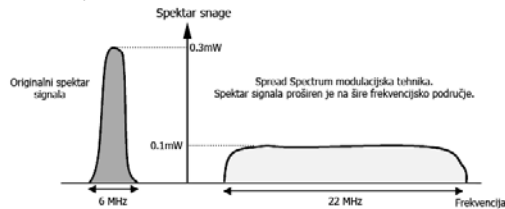
---

---

---

## 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 šuma
  - PN\*informacija = proširenje osnovnog spektra snage signala na šire frekvencijsko područje
- modulacija: FSK, GFSK, BPSK,...



B.Jeren i P.Pala: Sustavi za praćenje i vođenje procesa

Bežične mreže © 1991.-2008.

---

---

---

---

---

---

---

---

## Frekvencije: *Spread Spectrum*

- *Spread Spectrum* realizira se pomoću tehnika
  - FHSS
  - DSSS
  - DS/FHSS: hibrid FHSS i DSSS tehnike

B.Jeren i P.Pala: Sustavi za praćenje i vođenje procesa

Bežične mreže © 1991.-2008.

---

---

---

---

---

---

---

---

## Frekvencije: FHSS

- FHSS tehnika
  - eng. *Frequency Hopping Spread Spectrum*
  - frekvencijski opseg (ISM) podijeli se na 79 kanala širine 1MHz
  - tijekom emitiranja "skakanje" po frekvencijama po određenom slijedu
    - do 1600 puta u sekundi
    - zadržavanje informacije na određenom kanalu: *time slot* od 625us
  - ako nastane greška
    - emitira se ponovno na drugom kanalu
  - odašiljač i prijemnik upoznati sa slijedom preskakivanja radi održavanja veze
- koristi GFSK (*Gaussian Frequency Shift Keyeing*) modulaciju signala

B.Jeren i P.Pala: Sustavi za praćenje i vođenje procesa

Bežične mreže © 1991.-2008.

---

---

---

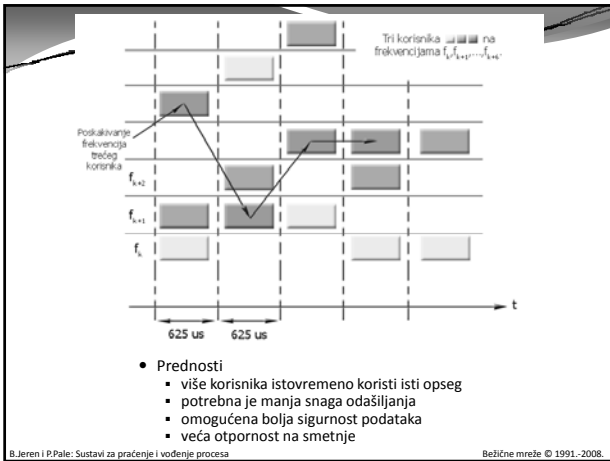
---

---

---

---

---




---

---

---

---

---

---

---

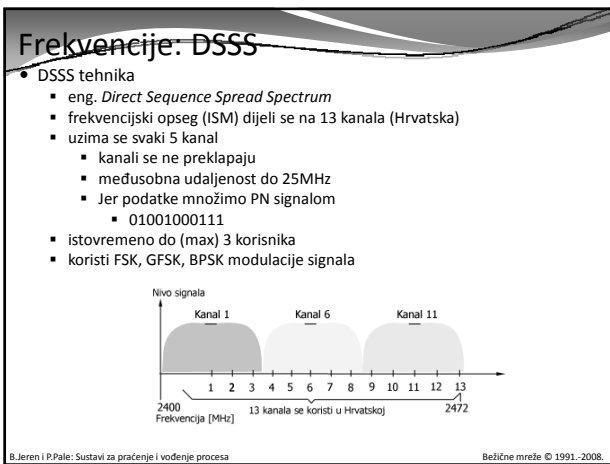
---

---

---

---

---




---

---

---

---

---

---

---

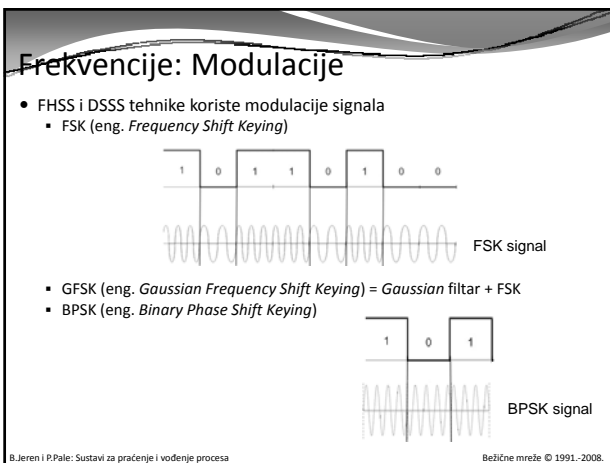
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

---

---

## 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

---

---

---

---

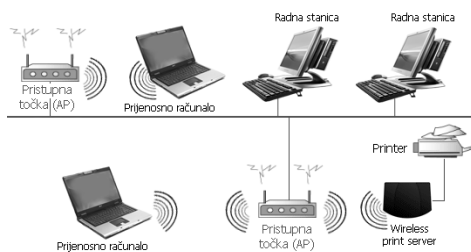
---

---

---

---

## Infrastrukturni način rada



- koristi se središnja pristupna točka
- svaki uređaj mora biti u dometu samo 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

B.Jeren i P.Pale: Sustavi za praćenje i vođenje procesa Bežične mreže © 1991.-2008.

---

---

---

---

---

---

---

---

---

---

## AP – Access Point

- središnja pristupna točka ili 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*

B.Jeren i P.Pale: Sustavi za praćenje i vođenje procesa Bežične mreže © 1991.-2008.

---

---

---

---

---

---

---

---

---

---

## AP root mode

- AP radi kao središnja pristupna točka
  - prima bežične klijente

B.Jeren i P.Pale: Sustavi za praćenje i vođenje procesa Bežične mreže © 1991.-2008.

---

---

---

---

---

---

---

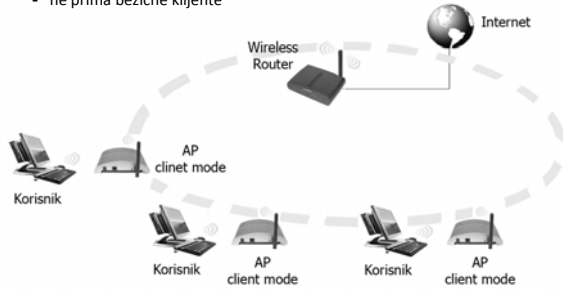
---

---

---

### AP client mode

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



---

---

---

---

---

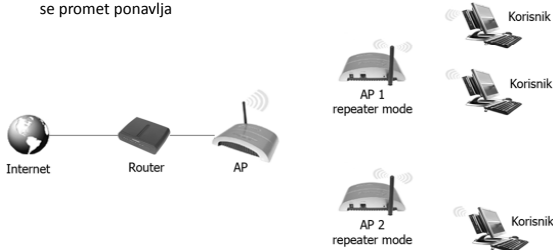
---

---

---

### AP repeater mode

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



---

---

---

---

---

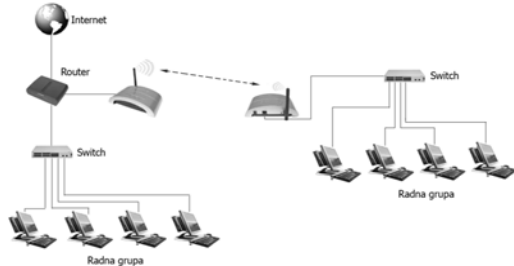
---

---

---

### 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 (eng. *Carrier Sense Multiple Access with Collision Avoidance*) protokol
  - 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

---

---

---

---

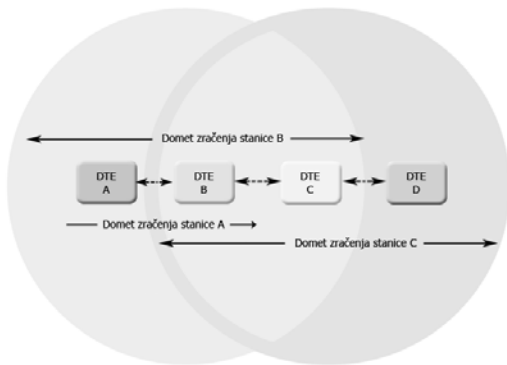
---

---

---

---

## Problem skrivene i izložene stanice



---

---

---

---

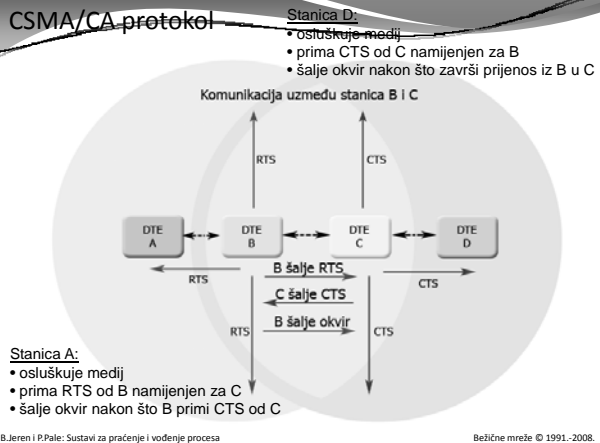
---

---

---

---

## CSMA/CA protokol



---

---

---

---

---

---

---

---



## Domet

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

---

---

---

---

---

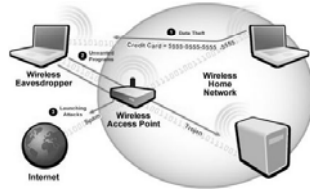
---

---

---

## 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
  - čekati da legitimni korisnik prestane s radom
  - ili istovremeno
    - napadati legitimnog korisnika
      - deauthentication, disassociation
    - predstavljati se u njegovo ime
- čak i kad se otkrije lažno predstavljanje
  - ne znamo gdje je napadač

---

---

---

---

---

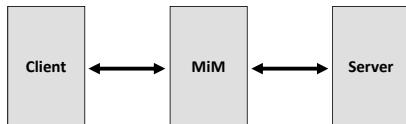
---

---

---

## 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

---

---

---

---

---

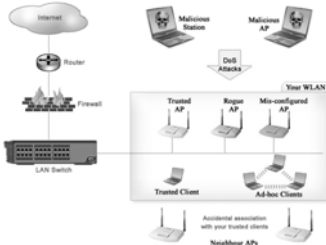
---

---

---

## 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 autentikacijski server -> RADIUS

---

---

---

---

---

---

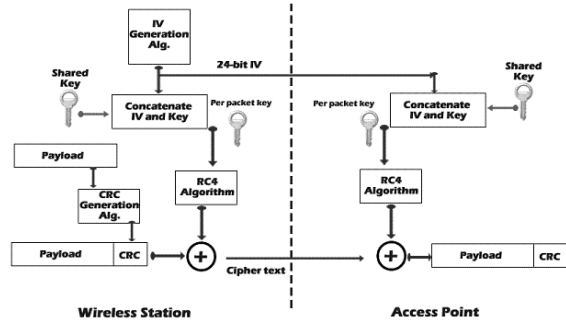
---

---

---

---

## WEP protokol – inicijalizacija veze




---

---

---

---

---

---

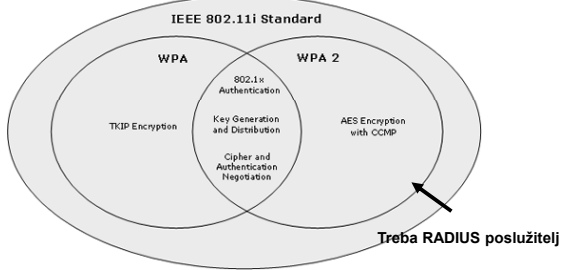
---

---

---

---

## 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

---

---

---

---

---

---

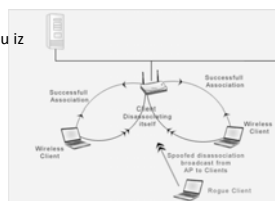
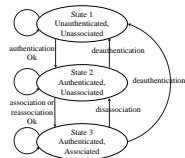
---

---

## 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 blokiran
- "deauthentication attack"
  - svi klijenti gube komunikaciju (ispadaju iz mreže)
- "authentication attack"
  - preplaviti AP "deauth" paketima
- i još ...
  - Time window attack
  - Virtual carrier sense attack




---

---

---

---

---

---

---

---

## 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

---

---

---

---

---

---

---

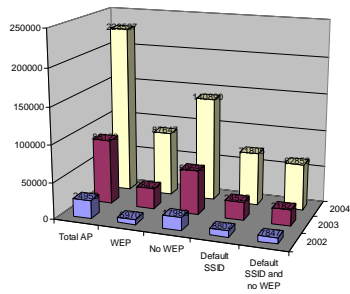
---

---

---

## Izloženost bežičnih mreža

Statistika ranjivosti bežičnih mreža



---

---

---

---

---

---

---

---

---

---