

Internet stvari

SVEUČILIŠTE U ZAGREBU



Diplomski studij Računarstvo

Znanost o mrežama Programsko inženjerstvo i informacijski sustavi

Računalno inženjerstvo

Informacijska i komunikacijska tehnologija

Automatika i robotika

Informacijsko i komunikacijsko inženjerstvo

Elektrotehnika i informacijska tehnologija

Audiotehnologije i elektroakustika Elektroenergetika

(Izborni predmet profila)

3. Komunikacijski protokoli za komunikaciju uređaja (sloj podatkovne poveznice): IEEE 802.15.4, 802.11ah, ZigBee, Z-Wave.

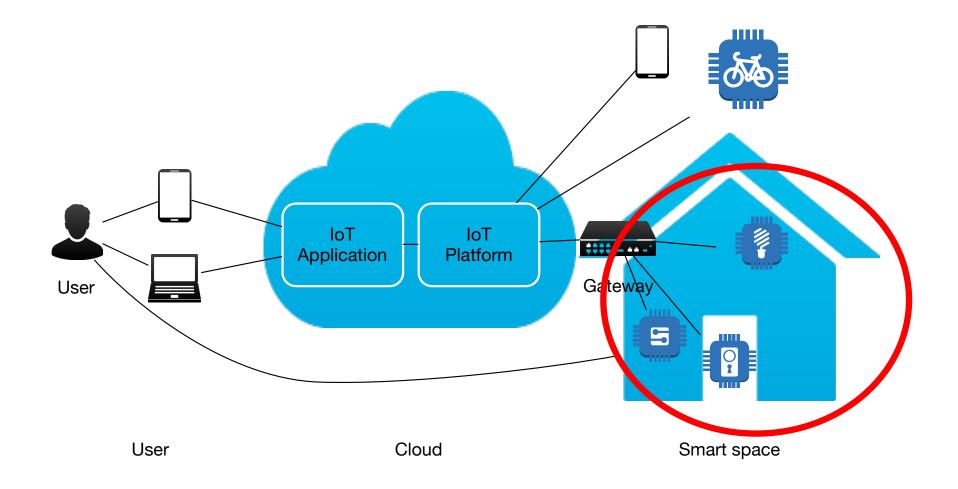
Ak. god. 2022./2023.

Sadržaj

- Bitna svojstva fizičkog sloja i podatkovne poveznice u IoT-u
- Standardi
- IEEE 802.15.4
- ZigBee
- Z-Wave
- IEEE 802.11ah



Arhitektura





Protokolni složaj IoT-a

TCP/IP

Aplikacijski

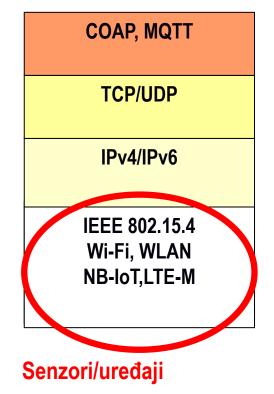
Transportni

Mrežni

Pod. povez.

Fizički

IoT



Pristup mreži Komunikacija uređaja M2M



Komunikacija uređaja

Zahtjevi

- što veći domet
- dugoročnost baterije (mala potrošnja, sleep mode)
- niska cijena uređaja
- jednostavno uvođenje u sustav
- podrška za masovnu primjenu
- malo komunikacijsko kašnjenje



Domet

Kratki

- IEEE 802.15.1 Bluetooth
 - na tijelu (BAN body area network)
 - certificirano da se može koristi u dodiru s tijelom
- IEEE 802.15.7 Visible Light Communications (VLC) FSO (free space optics)
 - nije zaživio u praksi

Srednji

- bežično: IEEE 802.11 Wi-Fi, IEEE 802.15.4, 802.15.4g/e, ZigBee, IEEE 802.11ah (na granici prema dugim), Z-wave, ...
- žično: IEEE 802.3 Ethernet, IEEE 1901.2 Narrowband Power Line Communications (PLC)

Dugi

- pokretna mreža: 2G 5G (NB-IoT)
- LPWA (Low-Power Wide-Area): LoRaWAN, Sigfox
- žično: IEEE 802.3xx optika (fiber), broadband (xDSL), IEEE 1901-2010 Broadband over PLC



Frekvencijski spektar (1)

- Nelicencirani spektar (ISM industrijski, znanstveni i medicinski):
 - 2.4 GHz koriste ga:
 - IEEE 802.11b/g/n Wi-Fi
 - IEEE 802.15.1 Bluetooth
 - IEEE 802.15.4 WPAN
 - Prednosti:
 - lakše postavljanje (ne trebaju licence)
 - veći kapacitet (brzina prijenosa)
 - Nedostaci:
 - interferencija (puno uređaja na tim frekvencijama)
 - zatvoreni prostor (zidovi, željezo, ...) smanjuje domet
 - veća potrošnja



Frekvencijski spektar (2)

- Uobičajene frekvencije ispod 1GHz za primjenu u IoT-u:
 - 169 MHz za brojila (struja, voda, plin, ...)
 - obično je potrebna dozvola
 - 433 MHz, 868 MHz (EU), 915 MHz (SAD)
 - obično se može koristiti za različite primjene: IEEE 802.15.4, IEEE 802.11ah, LoRaWAN, Sigfox, ...
 - 779–787 MHz samo u Kini
 - za IEEE 802.15.4g i LoRaWAN
- Prednosti:
 - veći domet
 - manja potrošnja energije
 - prolazi kroz zidove
- Nedostaci:
 - manji kapacitet
 - za neke je potrebna dozvola



Potrošnja energije

- Zahtjevi različiti za različite uređaje napajane baterijama:
 - 10-15 godina za brojila (voda i plin)
 - 5-7 godina za senzori pametnog parkinga
 - 2-3 godine za uređaje koji se mogu redovito održavati (npr. ENC)
- Kako to postići?
 - isključuju se pojedini dijelovi uređaja za vrijeme rada
 - uređaji "spavaju" (ne troše energiju ili troše vrlo malo)
 - bežične komunikacije koje troše puno manje energije
 - optimizirane komponente koje troše malo energije
- Kada nisu napajane baterijama isto to je problem potrošnje
 - npr. za Zagreb brojila 5-10W potrošnje, 300.000 kućanstava (voda, struja, plin) ~ 700.000 brojila → 3,5 MW potrošnje



Potrošnja energije – klasifikacija (1)

- RFC7228 https://tools.ietf.org/html/rfc7228
- Klase energetskog ograničenja

Ime	Vrsta ograničenja	Izvor energije
EO	O <mark>graničenj</mark> e događajem	Skupljanje energije iz događaja (npr. micanje)
E1	Ograničenje vremenskim periodom	Periodička zamjena ili punjenje (solarno)
E2	Ograničenje životnim vijekom	Nema zamjenjivih baterija (npr. ENC)
E3	Bez ograničenja	Priključeno na napajanje



Potrošnja energije – klasifikacija (2)

- RFC7228 https://tools.ietf.org/html/rfc7228
- Strategije korištenja energije za komunikaciju

Ime	Strategija	Mogućnost komunikacije
PO	Normalno je <mark>isključeno</mark>	Ponovno spajanje po potrebi. Glavna optimizacija je smanjiti energiju ponovnog spajanja.
P1	Niska potrošnja	Periodičko isključivanje. Povremeno uključivanje u mrežu (periodički). Potrebno podešavanje perioda.
P9	Uvijek uključeno	Cijelo vrijeme može komunicirati. Optimizacija sklopovlja (smanjenje frekvencije ili isključivanja pojedinih dijelova)



Topologija

- različite tehnologije mogu imati različite topologije
- osnovna podjela topologija:
 - zvijezda
 - svaki sa svakim (peer-to-peer)
 - stablo
 - mješovita (mesh)

- primjeri:
 - WiFi zvijezda oko AP-a (access point)
 - IEEE 802.15.4, IEEE 1901.2a PLC mješovito
 - neki čvorovi moraju primati tuđe poruke i slati ih dalje (relay)



IEEE 802.15.4

- Standard koji specificira bežične tehnologije prijenosa podataka za uređaje i mreže ograničenih mogućnosti s fokusom na nisku potrošnju energije
 - low-rate wireless personal area networks (LR-WPANs)
 - PHY & Medium Access Control (MAC)
- Frekvencijski pojas
 - 868.0-868.6 MHz (EU), 902-928 MHz (SAD), 2.4-2.485 GHz (svijet)
- Max brzina prijenosa: 250 kb/s
- Max snaga: ~1mW-100mW
- Okvir: 127 okteta



IEEE 802.15.4 - standardi

- Prvi standard 2003. (IEEE 802.15.4-2003), 2006., 2011., 2015.
 - Frekvencije i brzine:
 - 2,4GHz, 16 kanala, 250kb/s cijeli svijet
 - 915MHz, 10 kanala, 40kb/s Sjeverna i Južna Amerika
 - 868 MHz, 1 kanal, 20kb/s Europa, Bliski istok, Afrika
- Ostali standardi:
 - IEEE 802.15.4c-2009 frekvencije za Kinu (314-316 MHz, 430-434 MHz, 779-787 MHz)
 - IEEE 802.15.4d-2009 frekvencije za Japan (950 956 MHz)
 - IEEE 802.15.4f-2012 frekvencije 433 MHz
 - IEEE 802.15.4e-2012 podrška za ISA100.11a
 - IEEE 802.15.4g-2012 podrška za Smart Grid i frekvencije 902 928 MHz



IEEE 802.15.4

- Baza za ostale standarde:
 - ZigBee definira više slojeve
 - 6LoWPAN komprimirani IPv6 za prijenos preko IEEE 802.15.4
 - ZigBee IP evolucija ZigBeea da koristi 6LoWPAN i protokol usmjeravanja RPL
 - ISA100.11a industrijska automatizacija (temelji se na 6LoWPAN, IPv6 i UDP)
 - WirelessHART vremenski sinkronizirana, samoorganizirana i samozacjeljujuća mješovita arhitektura
 - Thread temelji se na 6LoWPAN/IPv6, sigurna i pouzdana mješovita mreža za kontroliranje proizvoda u kući



IEEE 802.15.4 – PHY – struktura paketa

Preambula	Graničnik početka okvira	Duljina okvira	PDSU (PHY Service Data Unit)
	cijsko zaglavlje okteta	PHY zaglavlje 1 oktet	0-127 okteta

Polja:

- Preambula (32 bitova) sinkronizacija
- Graničnik početka okvira (8 bitova)
- PHY zaglavlje (8 bits) duljina PSDU
- PSDU podaci



IEEE 802.15.4 – MAC – struktura paketa

Kontrola okvira	Broj sekvence	Odredište PAN ID	Odredišna adresa	Izvorište PAN ID	Izvorišna adresa	Sadržaj okvira	Frame Check Sequence
2 okt.	1 okt.		Adrese –	varijabilno	2 okt.		
MAC zaglavlje							MAC podnožje



IEEE 802.15.4: klase uređaja

- Full-function device (FFD)
 - Podržava sve mogućnosti
 - Može primati, slati i usmjeravati pakete
 - Koordinator, usmjeritelji moraju biti FFD
- Reduced-function device (RFD)
 - Ograničene komunikacijske i sklopovske mogućnosti
 - Krajnji čvor u mreži
 - Mogu trošiti malo energije i može spavati
 - Može komunicirati samo s FFD-ovima
 - Krajnji čvor može biti RFD (ili FFD)



IEEE 802.15.4 MAC: način rada

• Beacon-mode

- Koordinator upravlja i sinkronizira prijenos podataka
- Svi ostali čvorovi osluškuju *beacon* i potom koriste CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) za <mark>izbjegavanje sudara okvira</mark> nema osluškivanja prilikom transmisije, ako kanal nije slobodan čekaj *Random Backoff Time*
- Čvorovi mogu koristiti i pridijeljene vremenske odsječke za prijenos (GTS) koje im je dodijelio koordinator
- Omogućuje duty-cycling (čvorovi mogu ući u sleep mode radi smanjenja potrošnje energije)
- Non-beacon mode
 - Za komunikaciju od točke do točke
 - Čvorovi moraju kontinuirano osluškivati stanje na kanalu



IEEE 802.15.4 - sigurnost

- Enkripcijski algoritam Advanced Encryption Standard (AES)
 - ključ 128-bita
- Validacija integriteta primljenih podataka
 - Pomoću MIC-a (message integrity code) i AES-a
- U kontrolnom okviru se postavlja bit za sigurnost

Kontrola okvira	Broj sekvence	Odredište PAN ID	Odredišna adresa	Izvorište PAN ID	Izvorišna adresa	Dodatno zaglavlje sigurnosti	Sadržaj okvira	Frame Check Sequence
2 okt. 1 okt. Adrese – 4-20 okt.					0-14 okt	varijabilno	2 okt.	
MAC zaglavlje						MAC sac	Iržaj	MAC podnožje



ZigBee



- Preko 300 kompanija je sudjelovalo u njegovoj standardizaciji u sklopu ZibBee Alliance
- Temelji se na standardu IEEE 802.15.4
- Namijenjen primjenama koje zahtijevaju malu brzinu veze, nisku potrošnju energije, malo kašnjenje, sigurnu komunikaciju (128-bit AES encryption)
- Čvorovi se u nekoliko milisekundi mogu aktivirati iz uspavanog stanja
- Podržava 65 tisuća čvorova po mreži
- Uspostavljena mreža je vrlo robusna i otporna na kvarove
- Jednostavno upravljanje mrežom
- Brzine do 250kb/s



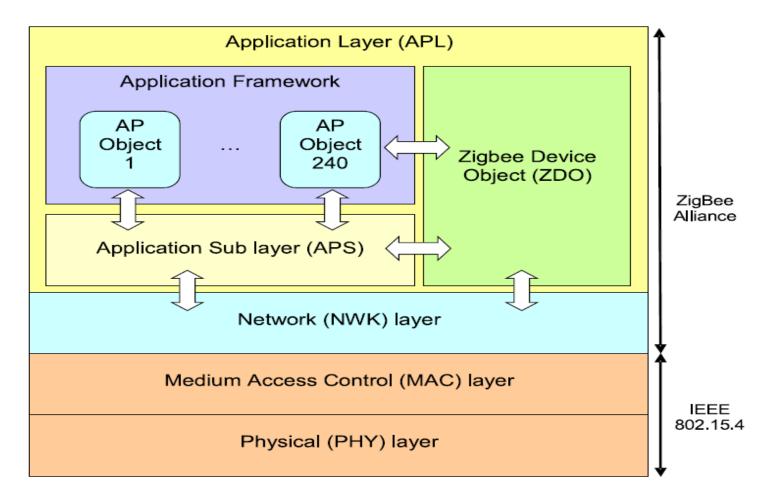
ZigBee - primjena

- Automatizacija zgrada sigurnost, HVAC, svjetla, brave, ...
- Osobno zdravlje nadzor pacijenata, fitness
- Industrijska automatizacija upravljanje resursima, kontrola okoline, upravljanje energijom
- Upravljanje domom sigurnost, HVAC, svjetla, brave, navodnjavanje travnjaka, ...
- Periferije računala miš, tipkovnica, joystick
- Potrošačka elektronika daljinski upravljači za TV, VCR, DVD/CD



ZigBee: Protokolni složaj

- NWK omogućuje sigurno višeskokovno usmjeravanje (koristi AODV), otkrivanje i održavanje putova, ulazak i napuštanje mreže te dodjeljivanje adresa novim čvorovima
- APL predstavlja okvir za razvoj raspodijeljenih aplikacija i komunikaciju
- ZDO omogućava međusobno otkrivanje APO-a i njihovu organizaciju u raspodijeljenu aplikaciju





Izvor: J. Brown: "Machine-2-Machine, Internet of Things, Real World Internet", 2011.

ZigBee – funkcije mrežnog sloja (NWK)

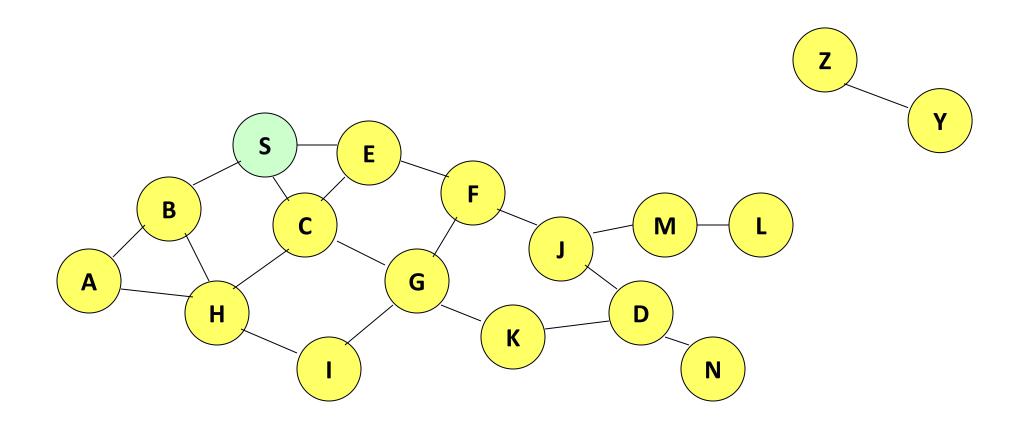
- Pokretanje mreže omogućuje uspostavu mreže
- Priključivanje i napuštanje mreže
- Konfiguracija mogućnost čvora da se konfigurira i radi u skladu s mrežom kojoj je pristupio
- Adresiranje koordinator dodjeljuje adrese čvorovima koji pristupaju mreži
- Sinkronizacija mogućnost sinkronizacije slušanjem beacona ili povlačenjem podataka
- Sigurnost očuvanje integriteta s kraja na kraj
- Usmjeravanje čvorovi mogu usmjeravati paketa do odredišta koristeći (AODV - Ad hoc On-Demand Distance Vector Routing)



ZigBee NWK – AODV usmjeravanje

- Ad Hoc On-Demand Distance Vector Routing (AODV)
- održava tablice usmjeravanja na putu među čvorovima koji žele komunicirati
- preplavljivanje porukama route request (RREQ) iz izvorišnog čvora S da bi se otkrio put do odredišta D
- čvor koji primi RREQ osvježava informaciju u tablici usmjeravanja
- kada D primi RREQ, odgovara sa route reply (RREP)
- put za isporuku paketa od S do D slijedi suprotan put od puta poruka RREP

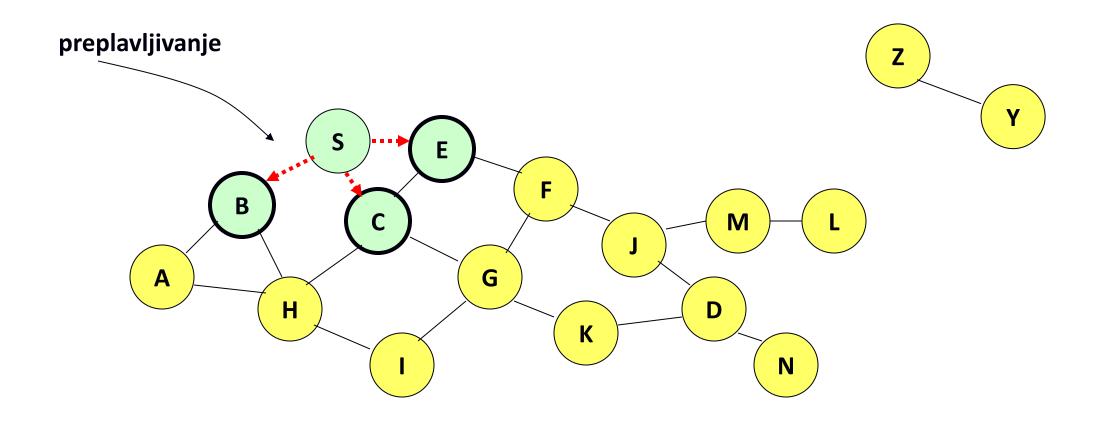






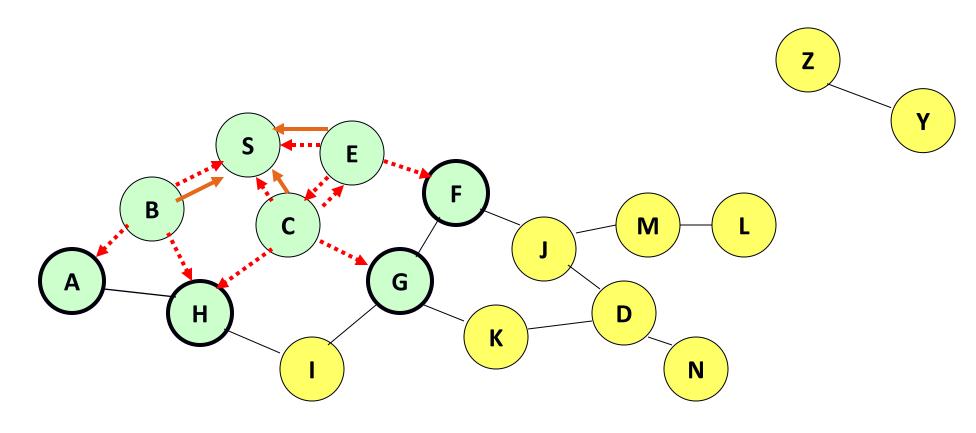
Oznaka čvora koji je primio RREQ za D od S





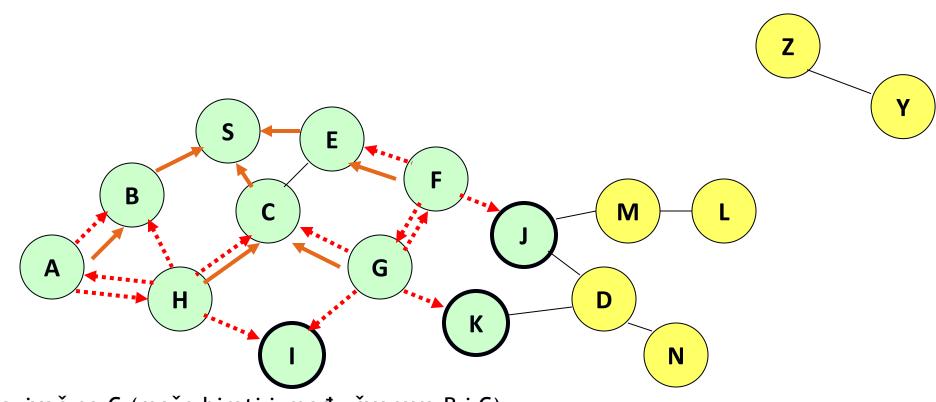
Prijenos Route Request (RREQ)





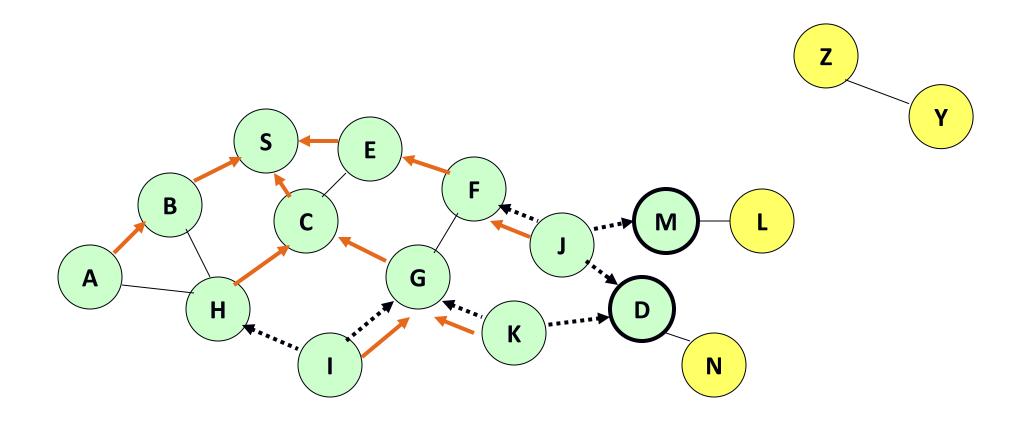
Oznaka pokazivača na prethodni čvor od koga je primljen RREQ



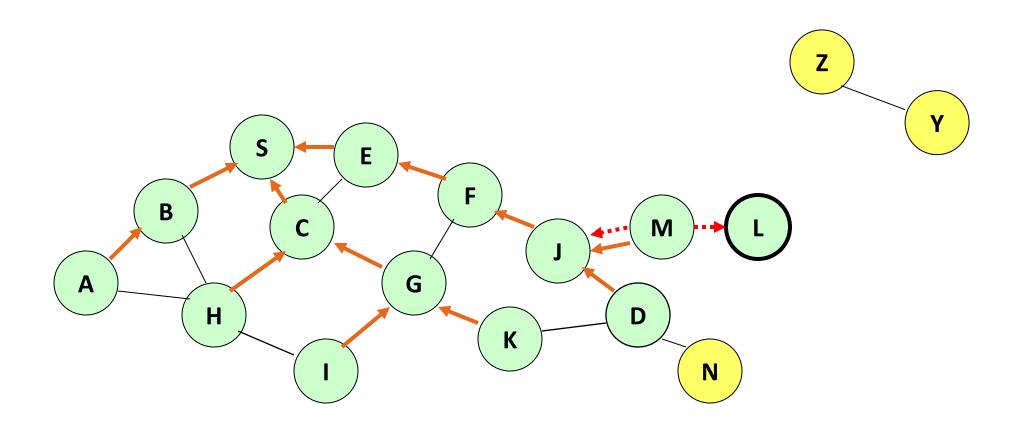


- •Čvor H definira pokazivač na C (može birati između čvorova B i C)
- •Čvor C prima RREQ od G i H, ali ga ne prosljeđuje ponovo, jer je C prethodno proslijedio isti RREQ (reagiraju samo I, J i K jer primaju RREQ prvi puta)





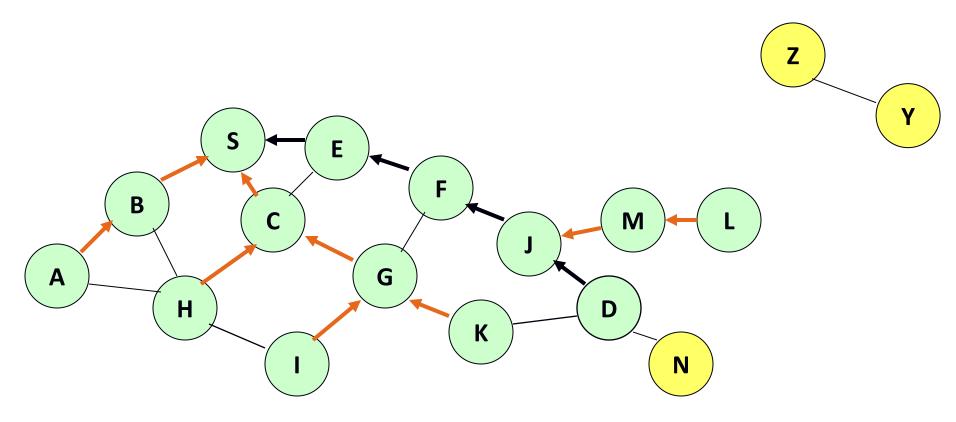




• Čvor D ne prosljeđuje RREQ dalje jer je D odredišni čvor



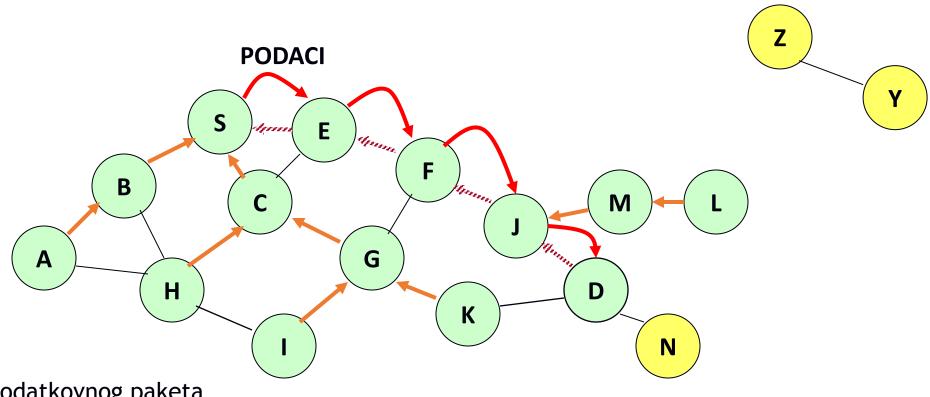
AODV – route reply



Prijenos poruke Route Reply (RREP) (slijedi pokazivače u svakom čvoru)



AODV – podatkovni paketi





Oznaka za put podatkovnog paketa Podaci slijede put suprotan od RREP (reverse path forwarding)



ZigBee – funkcije aplikacijskog sloja (APL)

- Zigbee Device Object (ZDO) održava što koji uređaj može što raditi (tablica) i obrađuje zahtjeve za povezivanje (bind)
- Postoje aplikacijski profili npr. Home Automation, Smart Energy
 - Opisuju kolekciju uređaja koji omogućuju aplikaciju i implicitno poruke
- Klasteri unutar profila
 - Funkcije unutar aplikacijskog profila npr. upravljanje svjetlom
- Krajnja točka (endpoint)
 - Komunikacijski entitet unutar uređaja npr. svjetlo u spavaćoj sobi je ep5
 - Jedan uređaj može imati više krajnjih točki
- Otkrivanje mogućnost otkrivanja koji drugi uređaj radi u području ovog uređaja
- Povezivanje (binding) mogućnost podudaranja 2 ili više uređaja koji pružaju usluge ili ih zahtijevaju te dozvoljavanje da komuniciraju



ZigBee - sigurnost

- Temelji se na AES-u (128-bitni ključevi)
- Definira sigurnost na slojevima: MAC, NWK, APS
- Sigurnost aplikacija je definirana kroz aplikacijske profile
- Trust centar
 - Čvor koji je zadužen za sigurnost. Obično koordinator.
 - Uloge:
 - Trust Manager autentifikacija uređaja koji se žele priključiti mreži
 - Network Manager održava i distribuira mrežne ključeve
 - Configuration Manager omogućuje sigurnost s kraja na kraj između uređaja



ZigBee - ključevi

- Master ključevi
 - Opcionalni su
 - Koriste se za inicijalnu razmjenu tajni između dva uređaja (SKKE Key Establishment Procedure za generiranje ključeva poveznice)
 - Ključevi iz Trust Centra se zovu Trust Center Master Keys
 - Ostali su Application Layer Master Keys
- Mrežni ključevi
 - Osiguravaju mrežu
 - Isti ključ imaju svi uređaji u mreži
 - Kod visoke sigurnosti se moraju prenositi kriptirano, a inače može i nekriptirano
- Ključevi poveznice (link)
 - Opcionalni su
 - Osiguravaju poruke na aplikacijskoj razini



Z-Wave



- Razvila ga privatna firma Zensys (2005.) Danska
 - kupila ih Sigma 2008., a prodani su Silicon Labsu 2018.
 - Jedini rade čipove
- Certifikacija kroz Z-Wave Alliance 1700 proizvoda od 300 proizvođača
 - Specifikacija je <u>ovdje</u>
- Primjena u pametnom domu
- Frekevencija <GHz (868 MHz Europa, 908 US)
- Maksimalna udaljenost 30-100m (ovisi o zaprekama) Z-Wave Plus 167m
- Brzina prijenosa: 9,6-100 Kb/s
- Koristi enkripciju AES 128
- Jedan uređaj može biti napajan 10 godina s baterijom veličine novčića



Z-Wave



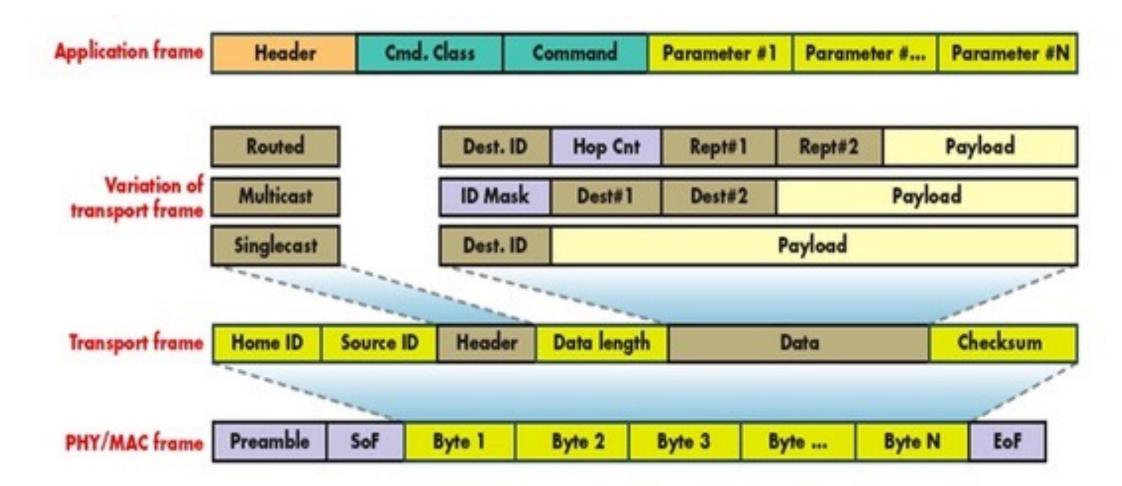
- Topologija mreže: Mesh, max. 232 uređaja u jednoj mreži
- Omogućuje maksimalno 4 prijenosa poruka u mreži
- Svaka mreža ima svoj Home ID dijeljen između uređaja
- Svaki uređaj ima svoj Node ID
- Vrste uređaja:
 - Controller ima postavljen Home ID i ne može se mijenjati u tvornici
 - Primarni i sekundarni kontroler
 - Slave prihvaćaju Home ID od primarnog kontrolera i kontroler im dodjeljuje Node ID
 - Može biti usmjeritelj u mreži
- Svaki čvor održava listu susjeda
- Načini slanja: single, multicast, broadcast
- Može se pokrenuti iscjeljivanje mreže gdje se ponovno posloži topologija



Z-Wave



39





IEEE 802.11ah

- Varijanta najpoznatijeg bežičnog protokola (WiFi)
- Standard objavljen 2016.
- Predviđena za IoT uređaje (lagana varijanta koja troši malo energije)
- Prilagodba za frekvencije ispod 1GHz
- Domet: do 1km
- Maksimalna brzina: 100 kb/s
- Redefiniran dio u fizičkom i MAC sloju



IEEE 802.11ah - primjena

- 3 najvažnija područja primjene:
 - Senzori i brojila
 - Npr. parkiranje, praćenje okoline/poljoprivreda, industrijski procesi, zdravlje i fitness, automatizacija zgrade
 - Agregacija podataka iz industrijskih postrojenja
 - Moguće povezivanje s podmrežom IEEE 802.15.4g
 - Proširivanje Wi-Fi-a na otvorenom prostoru



IEEE 802.11ah – fizički sloj (PHY)

- Koristi nelicencirana područja < 1GHz
 - 868–868.6 MHz EMEAR (Europa, Bliski istok, Afrika, Rusija)
 - 902–928 MHz Sjeverna Amerika, Azija i Pacifik
 - 314–316 MHz, 430–434 MHz, 470–510 MHz, 779–787 MHz Kina
- Koristi modulaciju OFDM
- Širina kanala:
 - 2, 4, 8, 16 MHz za računala, mobitele, ...
 - 1 MHz za malu propusnost (senzori)



IEEE 802.11ah – sloj podatkovne poveznice (MAC)

- Optimiran za frekvencije < 1GHz
- Omogućuje malu potrošnju
- Veći broj uređaja koji se mogu spojiti (8192 po AP-u)
- MAC zaglavlje smanjeno
- Grupiranje i sektorizacija sektorske antene
- Restricted access window (RAW) algoritam za izbjegavanje istovremenog slanja paketa
- Target wake time (TWT) AP može definirati kada se uređaj može spojiti → smanjena energija jer uređaj može u međuvremenu "spavati"



Pitanja za ponavljanje

- Navedite tehnologije kratkog/srednjeg/dugog dometa za komunikaciju uređaja u IoT-u.
- Usporedite prednosti i nedostatke nelicenciranog i licenciranog spektra.
- Koje su uobičajene frekvencije ispod 1GHz koje se koriste u IoT-u?
- Kako je moguće uštedjeti energiju kod IoT uređaja?
- Navedite i objasnite klase energetskog ograničenja.
- Navedite i objasnite strategije korištenja energije za komunikaciju.
- Navedite 4 mrežne topologije i gdje se koriste.
- Navedite 3 tehnologije koje koriste IEEE 802.15.4.

- Koja je razlika između FDD (full-function device) i RFD (reduced-function device) klasa uređaja u IEEE 802.15.4?
- Koja je razlika između sljedeća dva načina rada u IEEE 802.15.4: beacon-mode i non-beacon mode?
- Koji algoritam za šifriranje se koristi u IEEE 802.15.4?
- Što je ZigBee?
- Koje su funkcije mrežnog sloja (NWK) u ZigBeeu?
- Što je AODV i čemu služi?
- Koje vrste sigurnosnih ključeva postoje u ZigBeeu i čemu služe?
- Koje je razlika između ZigBeeja i Z-Wavea?
- Što je IEEE 802.11ah i koja su mu svojstva?

