

/Zavod za telekomunikacije

Diplomski studij

**Elektrotehnika i informacijska tehnologija, Informacijska i komunikacijska
tehnologija, Računarstvo**

Izborni predmet profila

Internet stvari

Akademska godina 2022./2023.

Ogledna pitanja s rješenjima - 1. blok predavanja

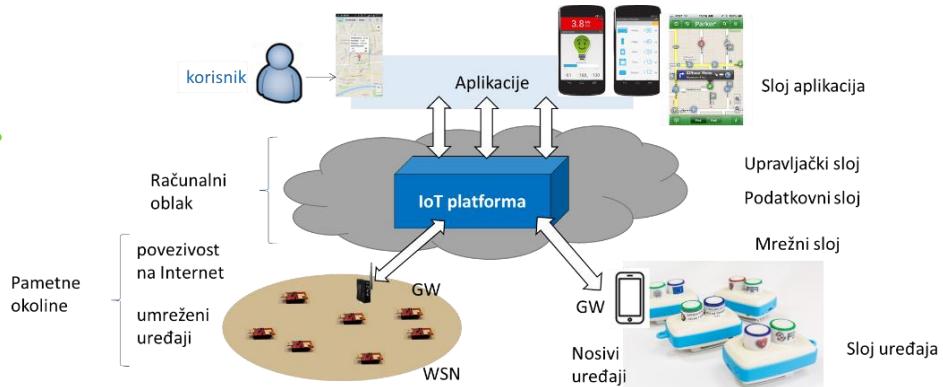


SVEUČILIŠTE U ZAGREBU

**Fakultet
elektrotehnike i
računarstva**

Zadatak 1

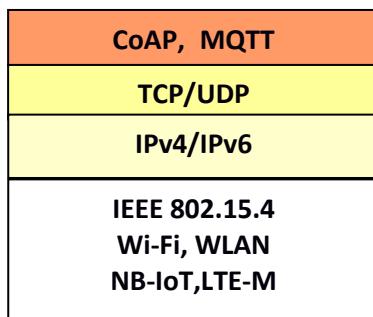
Skicirajte pojednostavljenu arhitekturu Interneta stvari. Objasnите funkcionalnosti pojedinih komponenti.



- **Nosivi uređaji, WSN (sloj uređaja)** – prikupljaju podatke o okolini (senzori) ili izvršavaju određene funkcije (aktuatori)
- **Mrežni sloj** – omogućuje komunikaciju između IoT-uređaja i računalnog oblaka za pohranu podataka
- **Računalni oblak (podatkovni i upravljački sloj)** – pohranjuje podatke prikupljenje sa IoT-uređaja, izvršava analizu podataka, omogućuje upravljanje IoT-uređajima (odabir vremena aktivnosti, podataka koji se prenose)
- **Aplikacije (aplikacijski sloj)** – omogućuju prikaz podataka krajnjim korisnicima

Zadatak 2

Skicirajte protokolni složaj za Internet stvari. Navedite pune nazine za barem dva karakteristična protokola za Internet stvari. Pojasnite osnovne značajke svakog sloja.



CoAP: Constrained Application Protocol

MQTT: Message Queuing Telemetry Transport

Sloj podatkovne poveznice omogućuje povezivanje IoT-uređaja na mrežu.

Mrežni sloj omogućuje adresiranje IoT-uređaja spojenih preko drugih fizičkih mreža te usmjeravanje prometa između različitih fizičkih mreža. Transportni sloj je zadužen za prijenos aplikacijskog prometa preko komunikacijske mreže i isporuku paketa odgovarajućim procesima na računalima. Aplikacijski sloj je zadužen za prijenos senzorskih i aktuatorских podataka između IoT-uređaja te poslužitelja i krajnjih korisnika.

Zadatak 3

Navedite namjenu uređaja kojeg nazivamo „senzor“ u kontekstu Interneta stvari te nabrojite komponente od kojih se sastoji senzorski čvor.

*Senzor: uređaj za opažanje fenomena iz okoline, malih je dimenzija, troši мало energije (baterija), te posjeduje ograničene resurse.
Sastoji se od komponenti za opažanje i mjerjenje fenomena iz okoline, procesora i memorije te komponente za komunikaciju.*

Zadatak 4

Grupirajte sljedeće bežične komunikacijske tehnologije prema dometu:
ZigBee, LoRaWAN, IEEE 802.15.4 XBee, IEEE 802.15.1 Bluetooth, IEEE 802.11 Wi-Fi, IEEE 802.15.7 Visible Light Communications (VLC), NB-IoT, Sigfox

Kratki	Srednji	Dugi
IEEE 802.15.1 Bluetooth, IEEE 802.15.7 Visible Light Communications (VLC)	ZigBee, IEEE 802.15.4 XBee, IEEE 802.11 Wi-Fi,	LoRaWAN, NB-IoT, Sigfox

Zadatak 5

Zaokružite LPWAN (*Low-power wide-area network*) tehnologiju s najboljim karakteristikama za:

Skalabilnost Sigfox LoRaWAN **NB-IoT**

Domet **Sigfox** LoRaWAN NB-IoT

Kašnjenje Sigfox LoRaWAN **NB-IoT**

• •

Zadatak 6

Navedite i objasnite namjenu protokola 6LoWPAN (*IPv6 over Low-Power Wireless Personal Area Networks*) te nabrojite tri mehanizma prilagodbe koje ovaj protokol koristi.

Optimizacija prijenosa IPv6-paketa u mrežama s ograničenim resursima (IEEE 802.15.4)

- Najmanji maximum transmission unit (MTU) za IPv6 je 1280 byte-a, dok je 127 byte-a najveći MTU za IEEE 802.15.4
- Potrebni su mehanizmi prilagodbe:
- Kompresija zaglavja
- Fragmentacija paketa
- Mesh-adresiranje

Zadatak 7

Navedite namjenu protokola RPL (*IPv6 Routing Protocol for Low Power and Lossy Networks*) te objasnite dva načina rada ovog protokola.

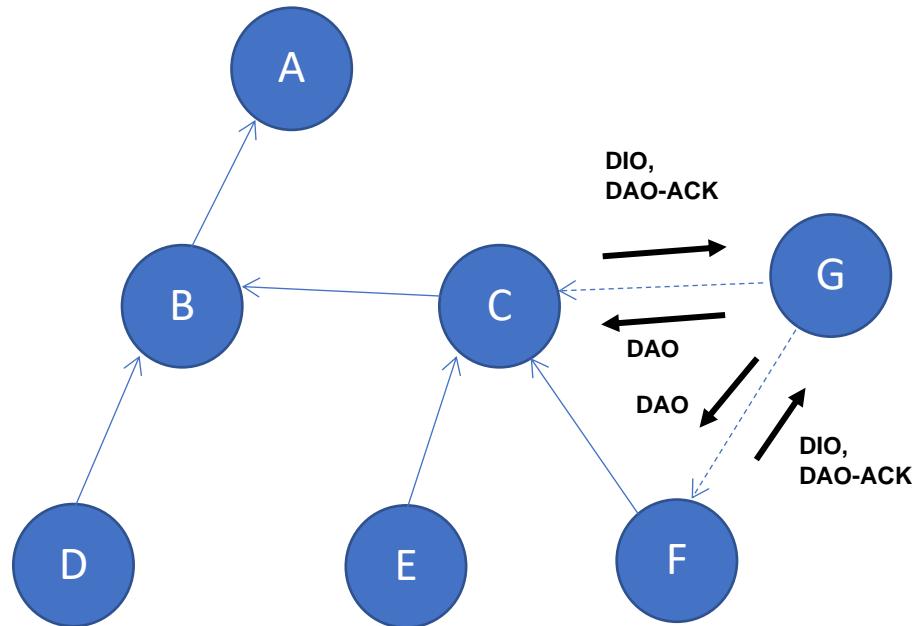
- Novi protokol za usmjeravanje paketa u mrežama ograničenih resursa (*distance-vector routing protocol*)
- **Storing mode:** Svi čvorovi sadrže potpunu tablicu usmjeravanja za jednu RPL domenu. Svaki čvor zna odrediti put prema svim ostalim čvorovima.
- **Non-storing mode:** Samo rubni usmjeritelji (*border router/s*) RPL domene sadrži potpunu tablicu usmjeravanja i zna odrediti put do krajnjeg čvora. Svi ostali čvorovi održavaju samo listu roditelja za usmjeravanje prema rubnom usmjeritelju.
 - Učinkovito rješenje na nivou čvora (štedi memoriju i CPU), ali koji su nedostaci?

Zadatak 8

Na slici su prikazani čvorovi mreže u kojoj se usmjeravanje izvršava korištenjem protokola RPL (IPv6 Routing Protocol for Low Power and Lossy Networks).

Naznačite na slici poruke koje se razmjenjuju nakon što se čvor G uključi u mrežu. Čvor G ima mogućnost komuniciranja s čvorom C i s čvorom F. Koji čvor će biti odabran kao roditeljski čvor čvora G? Zašto?

Kao preferirani roditeljski čvor bit će odabran čvor C zbog povoljnijeg ranga (2). Rang predstavlja broj skokova do korijenskog čvora.



Prikažite tablicu usmjeravnja na čvor B za Storing i Non-storing način rada.

Storing način rada:

Destination	Next hop	Metrics
C	C	1
D	D	1
E	C	2
F	C	2
G	C	2

Non-storing način rada: samo rubni usmjeritelj (A) ima tablicu usmjeravanja

Zadatak 9

U pametnom domu su dostupne dvije vrste senzora te dvije vrste aktuatora u dvije različite prostorije. Senzori omogućuju mjerena temperature i razine osvjetljenja. Aktuatori omogućuju uključivanje i isključivanje sustava za grijanje te upravljanje osvjetljenjem. Mjerena sa senzora te stanje aktuatora (jesu li sustavi kojima aktuatori upravljaju uključeni ili isključeni) se objavljaju korištenjem MQTT klijenta-objavlјivača.

- a) Definirajte teme na koje se objavljaju senzorska mjerena i stanja aktuatora tako da je moguće pretplaćivanje na svaki resurs po tipu (senzor/aktuator) i po lokaciji.

Apartment/room1/sensor/temp
Apartment/room1/sensor/lum
Apartment/room1/actuator/lighting
Apartment/room1/actuator/heat

Apartment/room2/sensor/temp
Apartment/room2/sensor/lum
Apartment/room2/actuator/lighting
Apartment/room2/actuator/heat

- b) Prikažite format pretplate za slučaj kada se MQTT klijent pretplatnik pretplaćuje na primanje svih dostupnih vrijednosti sa senzora

Apartment/+sensor/#

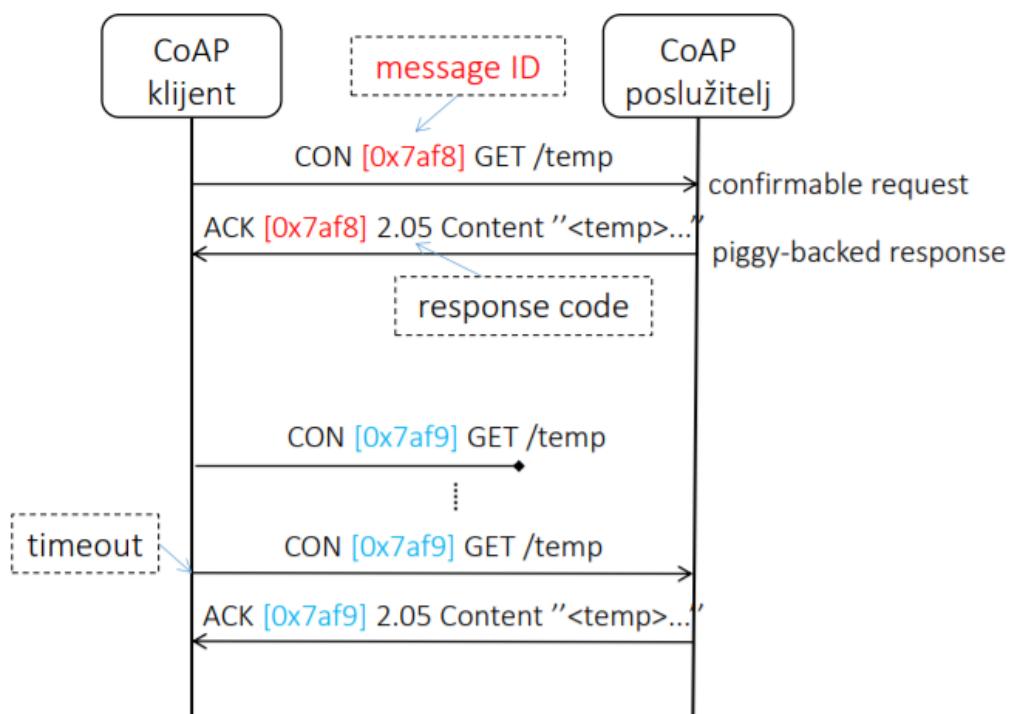
- c) Prikažite format pretplate za slučaj kada se MQTT klijent pretplatnik pretplaćuje na primanje svih dostupnih vrijednosti iz sobe 1

Apartment/room1/#

**Zadatak
10**

Skicirajte primjer razmjene poruka između CoAP klijenta i CoAP poslužitelja za *confirmable request* u slučaju a) ispravnog prijenosa klijentskog zahtjeva i b) neispravnog prijenosa klijentskog zahtjeva kada se na strani klijenta dogodi *timeout*.

Zapišite proizvoljne vrijednosti *message ID* za poruke koje se razmjenjuju. Koje poruke imaju isti *message ID*?



**Zadatak
11**

Navedite nekoliko značajnih problema vezanih uz sigurnost i privatnost u IoT-u.

- Fokus je na *funkcionalnosti uređaja/sustava*
- Fokus je na *sučeljima prema korisnicima*
- Pokušava se *skratiti vrijeme razvoja* radi što ranijeg izlaska na tržište
- Napadači poznaju tehnologije i imaju alate za automatizirani napad na pojedine slojeve/tehnologije
- Razvijatelji nisu sigurnosni stručnjaci (ne postoje gotova rješenja niti metodologije za implementaciju sigurnosti)
- Razvijatelji razvijaju komponente i integriraju ih u sustav, ostavljaju veliku površinu za napade preko cijelog složaja

**Zadatak
12**

Zaokružite točan odgovor.

1. Korištenjem protokola MQTT (*Message Queuing Telemetry Transport*) moguće je definirati preplatu koja obuhvaća više tema.

- a) DA
- b) NE

2. Razina kvalitete usluge korištenjem protokola MQTT koja uključuje isporuku poruke barem jedan put, pri čemu je moguće primanje više od jedne poruke je:

- a) Razina 0
- b) **Razina 1**
- c) Razina 2
- d) Razina 3

3. U zadaće MQTT poslužitelja (brokera) ne ubraja se:

- a) prihvatanje konekcije od strane klijenta
- b) proslijeđivanje poruke klijentima koji su pretplaćeni na temu na koju je poruka objavljena
- c) **objavljivanje nove poruke na postojeću temu**
- d) odgovaranje klijentu na PING zahtjev

4. Protokol CoAP (*Constrained Application Protocol*) na transportnom sloju koristi protokol:

- a) **UDP (User Datagram Protocol)**
- b) TCP (*Transmission Control Protocol*)
- c) SCTP (*Stream Control Transmission Protocol*)
- d) SIP (*Session Initiation Protocol*)

5. Metoda koja je podržana protokolom HTTP, ali nije podržana protokolom CoAP je:

- a) GET
- b) POST
- c) DELETE
- d) **OPTIONS**



SVEUČILIŠTE U ZAGREBU



Fakultet
elektrotehnike i
računarstva

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)

Internet stvari

**1. Općenito o Internetu stvari:
osnovni pojmovi, arhitektura
i područja primjene**

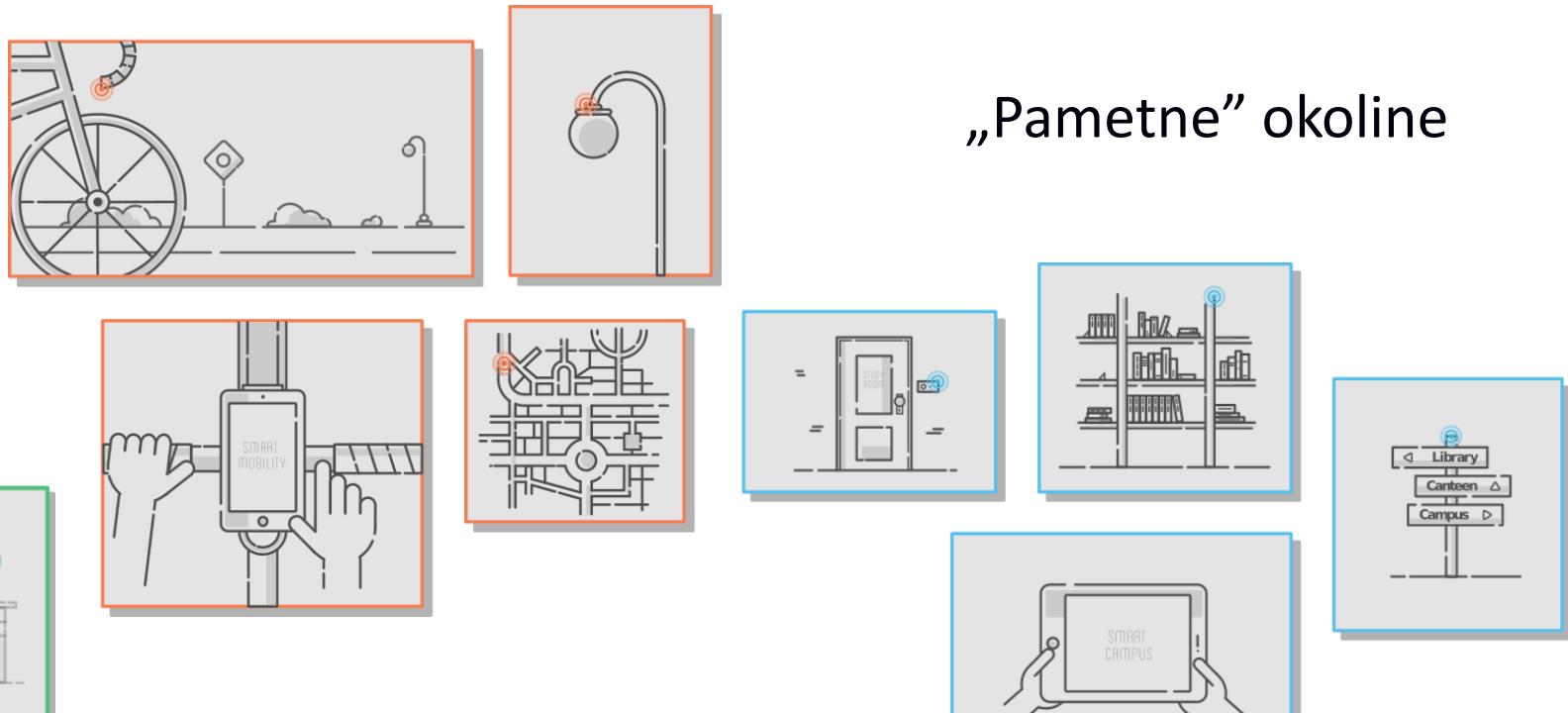
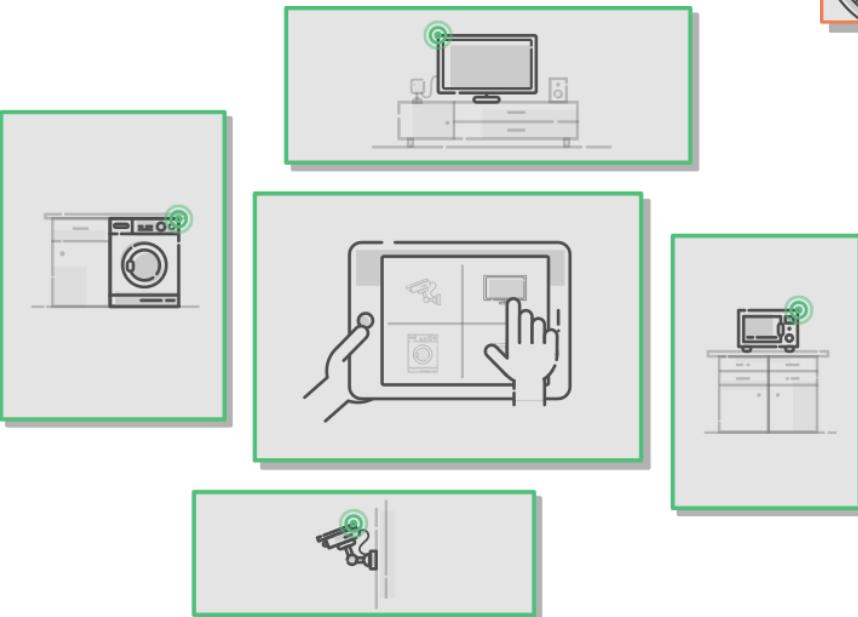
Ak. god. 2022./2023.

Sadržaj

- Umreženi uređaji i Internet stvari (engl. *Internet of Things*, IoT)
- Područja primjene
- Programske platforme za IoT
- Referentne arhitekture

IoT danas

Veliki broj umreženih heterogenih uređaja

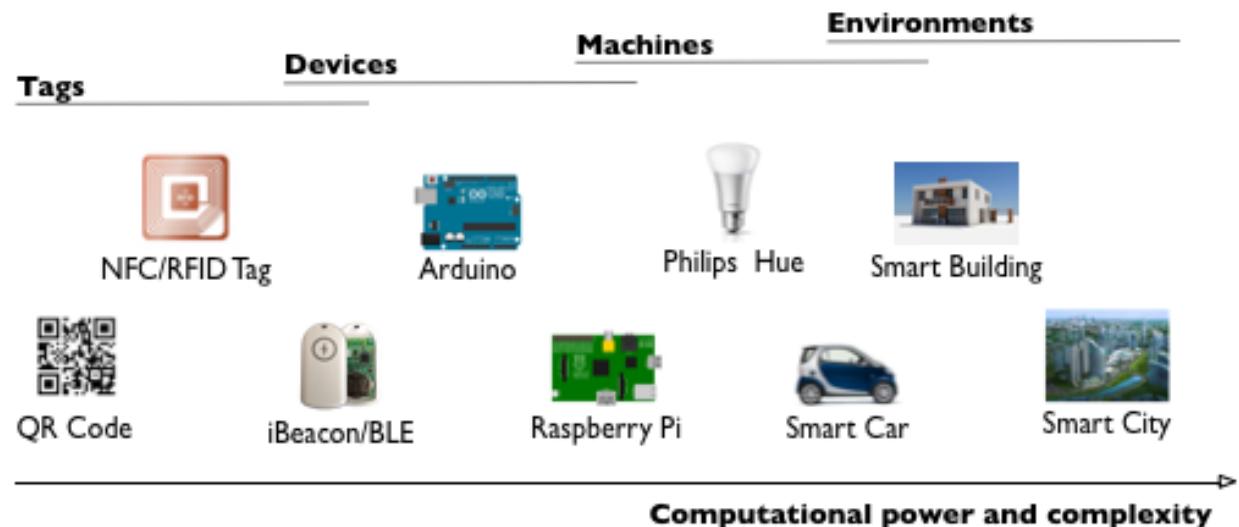


„Pametne“ okoline

Specijalizirane programske platforme: ~400

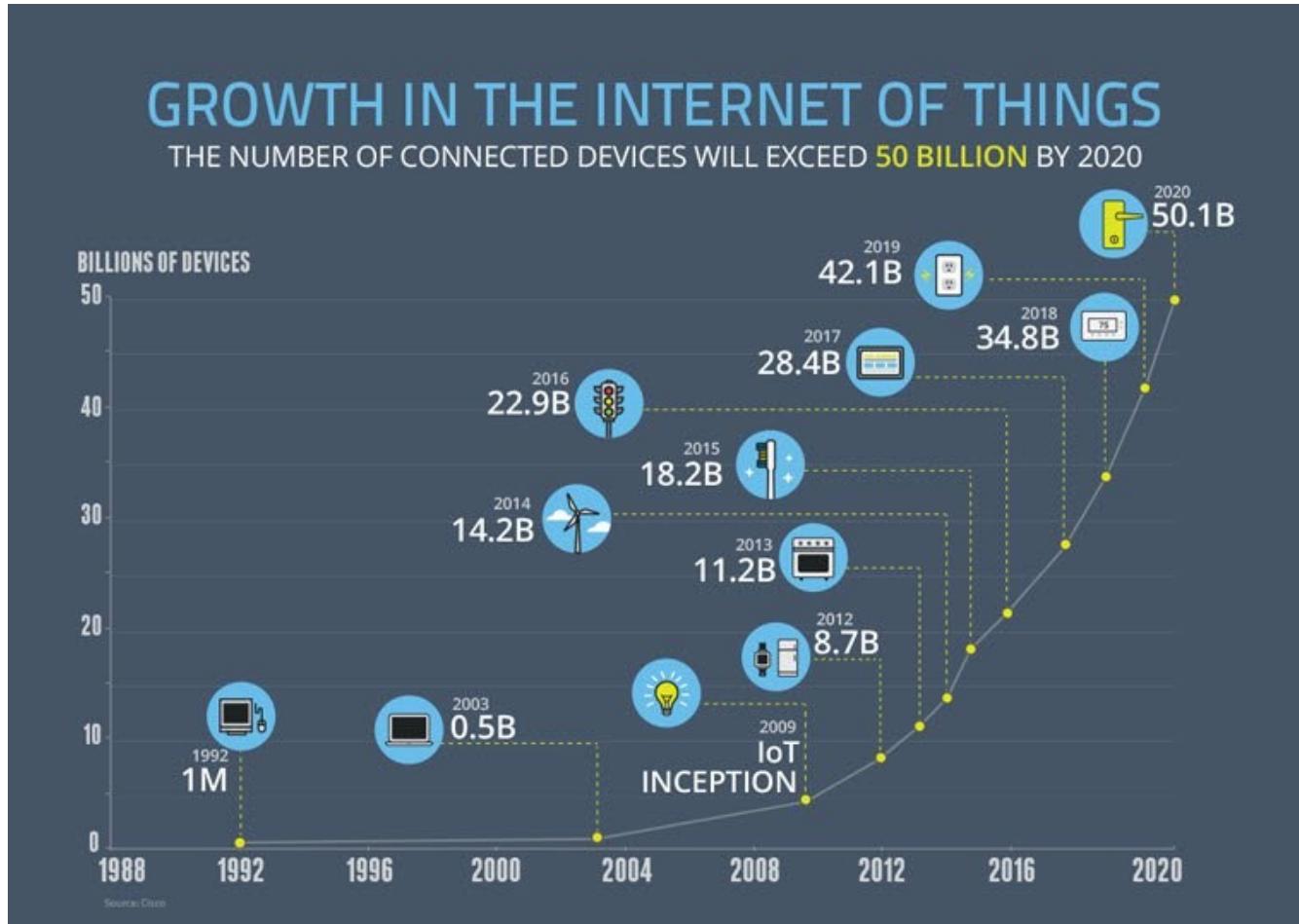
Umreženi uređaj („stvar”)

- Objekt iz fizičkog svijeta ili virtualnog digitalnog svijeta (virtualni objekt)
 - ima jedinstveni identifikator i povezan je na Internet (direktno ili putem posrednika)
 - senzor: opažanje okoline, potencijalno kontinuirano generira podatke
 - aktuator: može izvršiti određene funkcije



Source: Building the Web of Things: book.webofthings.io
Creative Commons Attribution 4.0

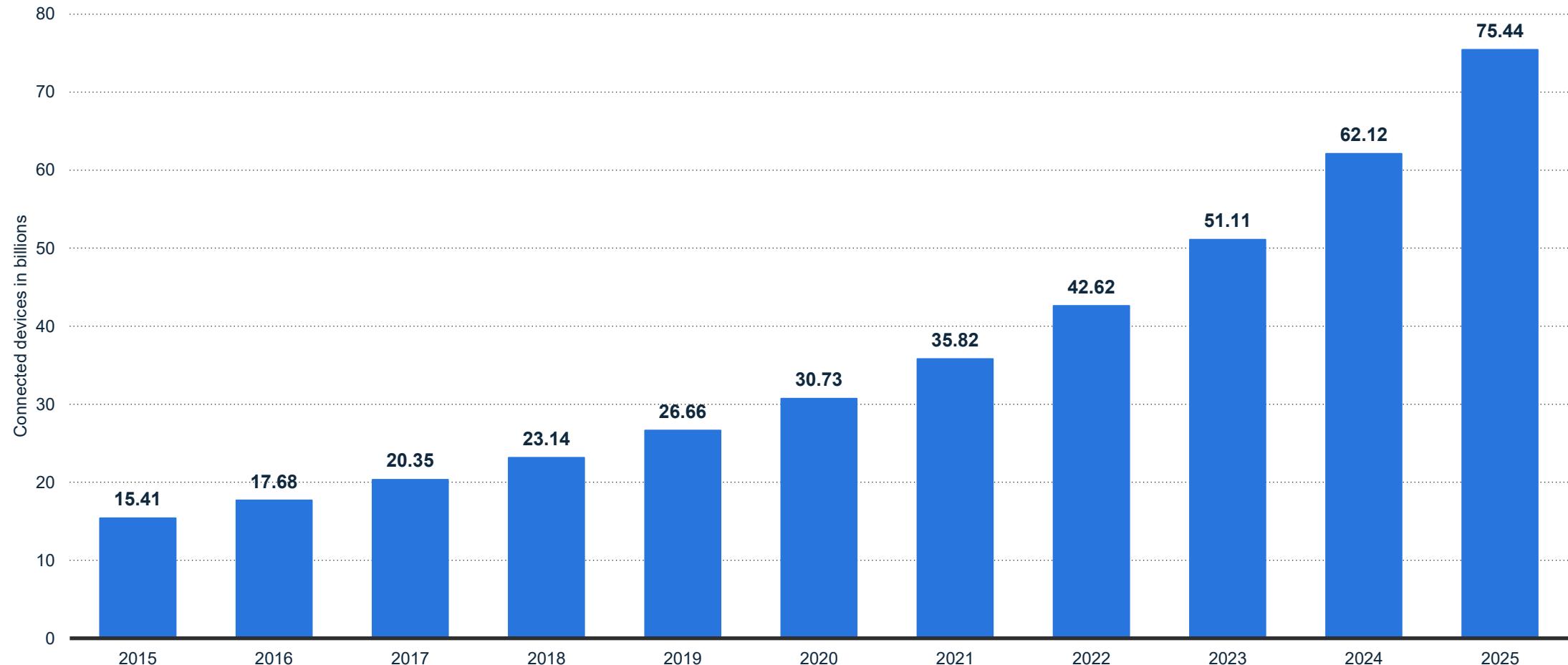
Broj stvari povezanih na Internet



Izvor: Cisco Internet of Things Infographic (2016)

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)

Internet of Things - number of connected devices worldwide 2015-2025



Kako smo stigli do IoT-a?

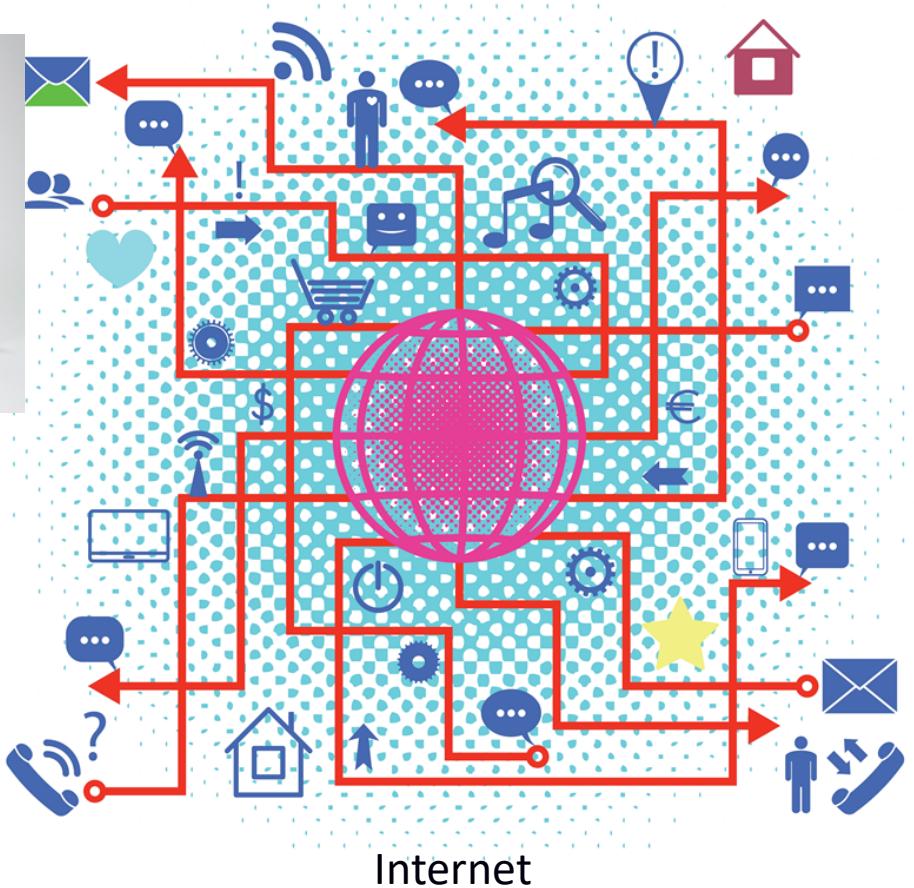


minijaturizacija el. sklopova,
smanjena potrošnja energije



pokretne mreže (4G)
i pametni telefoni

bežične senzorske mreže
Wireless Sensor Networks (WSN)



Internet of Things (IoT): definicija

ITU-T Recommendation Y.2060, 06/2012:

- *A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) Things based on, existing and evolving, interoperable information and communication technologies.*
 - *Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.*
 - *In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.*

Područja primjene

Smart Home

- Smart Lighting
- Smart Appliances
- Intrusion Detection
- Smoke/Gas Detectors
- Energy Management

Smart City

- Smart Parking
- Waste Management
- Smart Lighting
- Emergency Response

Environment

- Weather Monitoring
- Air Pollution Monitoring
- Noise Pollution Monitoring
- Forest Fire Detection

Retail

- Inventory Management
- Smart Vending Machines
- Smart Payments

Logistics

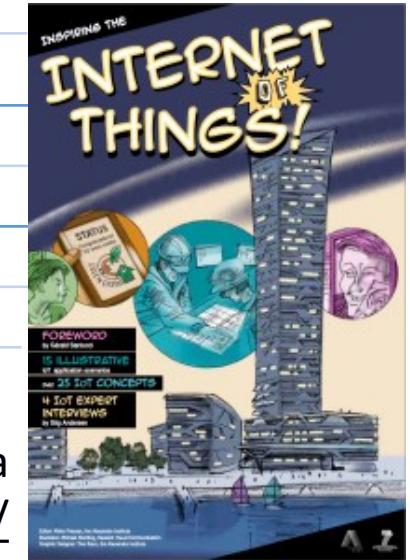
- Fleet Tracking
- Shipment Monitoring
- Remote Vehicle Diagnostics
- Route Generation and Scheduling

Industry

- Machine Diagnosis
- Object Tracking and Process Automation

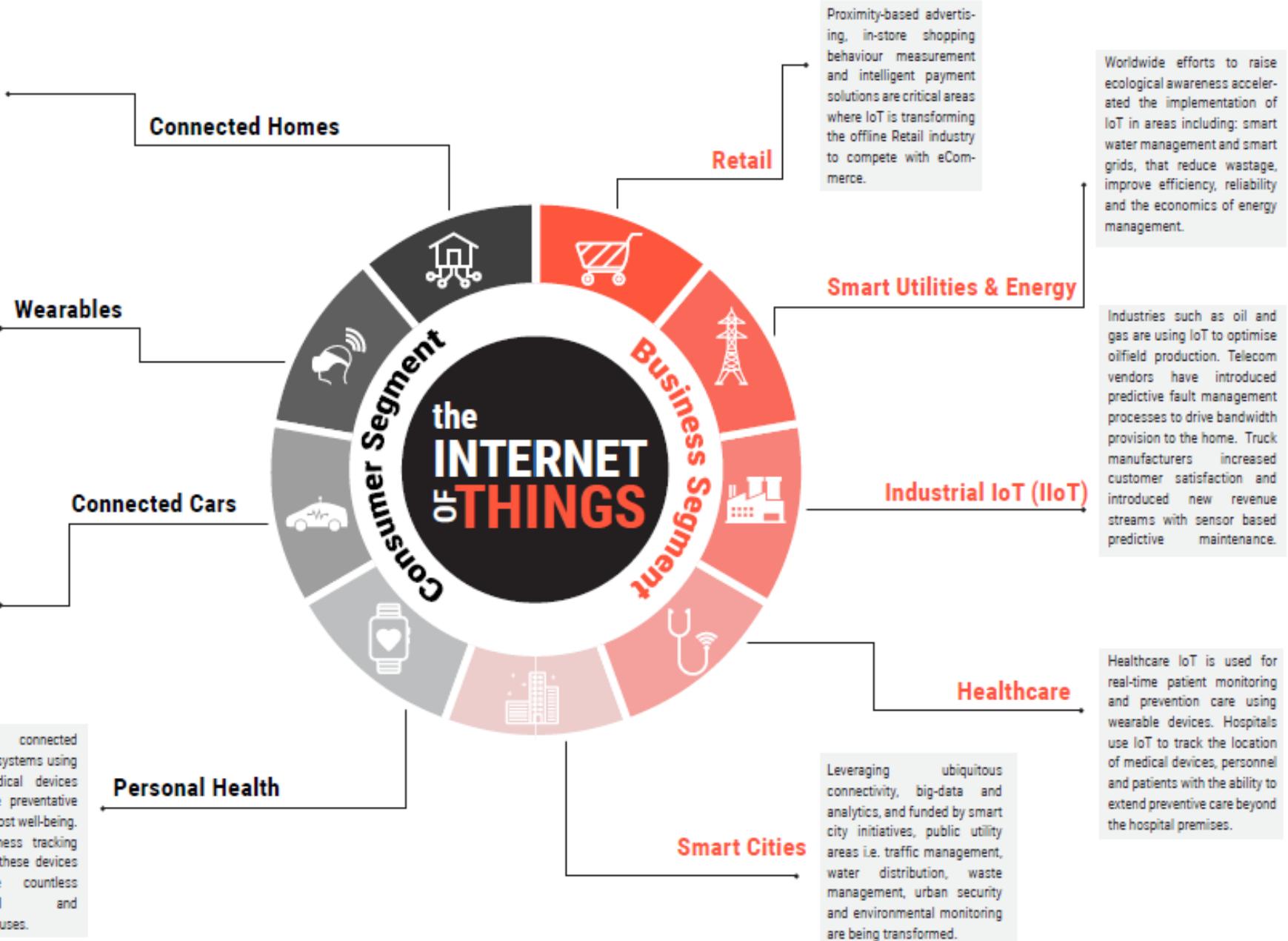
Agriculture

- Smart Irrigation
- Crop Monitoring



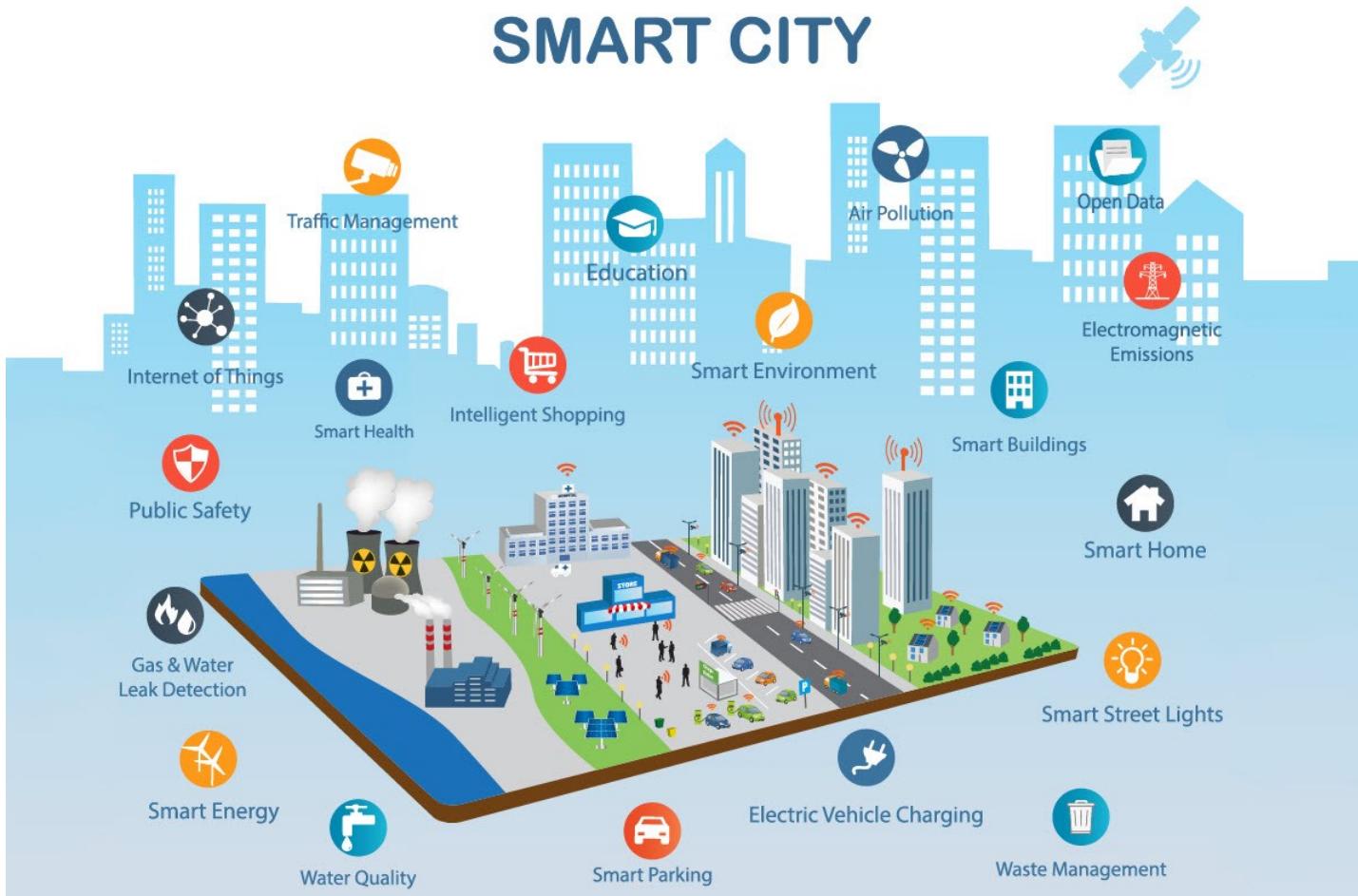
Za ljubitelje stripova

<http://iotcomicbook.org/original-edition/>



Izvor:
 Statista,
 Market Pulse
 Report IoT,
 April 2017

Koncept pametnog grada



Umreženi uređaji i inovativne IKT usluge su pokretači razvoja održivih i tehnološki naprednih gradova u službi građana i gradskih službi.

- ◆ Javni prijevoz
- ◆ Parkiranje
- ◆ Gradski promet
- ◆ Zbrinjavanje otpada
- ◆ Mjerenje buke, kvalitete zraka
- ◆ Pametna rasvjeta
- ◆ Energetska učinkovitost
- ◆ Nadzor prometnica
- ◆ Upravljanje prometom

Kako integrirati "stvari" i ponuditi inovativne aplikacije korisnicima?

- Pomoću programskih platformi (**IoT-platforma**) koje integriraju i upravljaju uređajima
 - uređaji: često imaju vrlo ograničene resurse te su povezani na Internet putem prilaznog uređaja (engl. *gateway*)
 - potrebno je objediniti i na jedinstveni način zapisati podatke primljene iz različitih izvora
 - potreba za obradom velike količine podataka (često u stvarnom vremenu)
 - raspodijeljeni sustav velikih razmjera
 - *Web of Things*: koncept koji povezuje uređaje direktno na WWW (tehnologije vezane uz protokol HTTP)

Business Value

Data Analytics

Core Platform

Connectivity

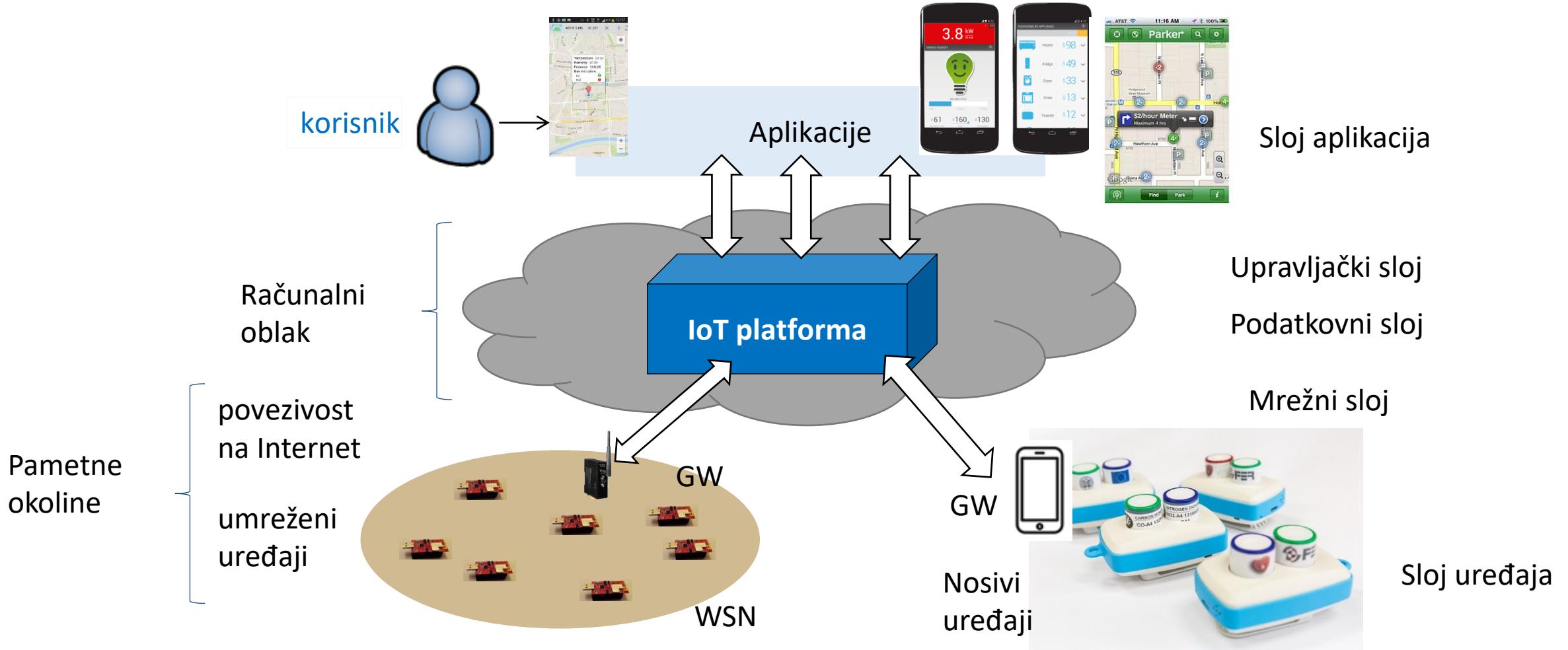
Thing

High-level IoT Stack

Okolina IoT-a

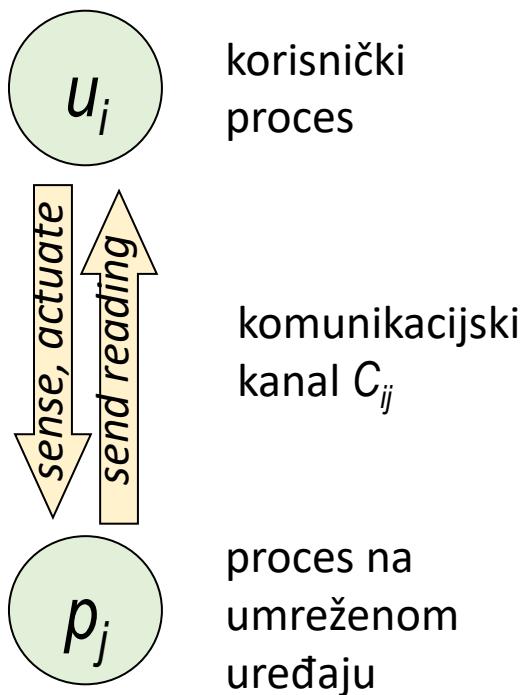
- pametna okolina integrira veći broj umreženih uređaja pomoću jedinstvene programske platforme kako bi se korisniku ponudile inovativne aplikacije (mobilne ili web aplikacije), npr. pametna kuća/ured/tvornica, pametan kampus, itd.
- računani oblak: pohrana i obrada podataka iz pametne okoline
- danas su na raspolaganju pretežno izolirana rješenja jednog ponuđača usluge u području IoT koji postavlja i integrira infrastrukturu u „pametnoj okolini”, podaci iz pametne okoline prikupljaju se u računalnom oblaku, pametnom okolinom se upravlja iz računalnog oblaka, a korisniku nude mobilne/web aplikacije za upravljanje vlastitom pametnom okolinom

Pojednostavljena arhitektura Interneta stvari



Generički model (osnovni) IoT-sustava

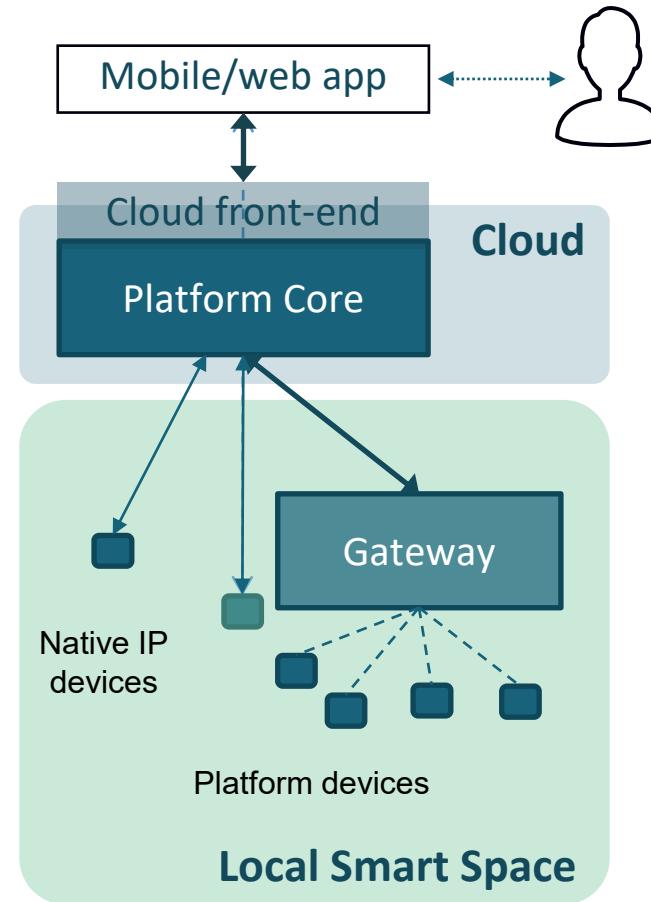
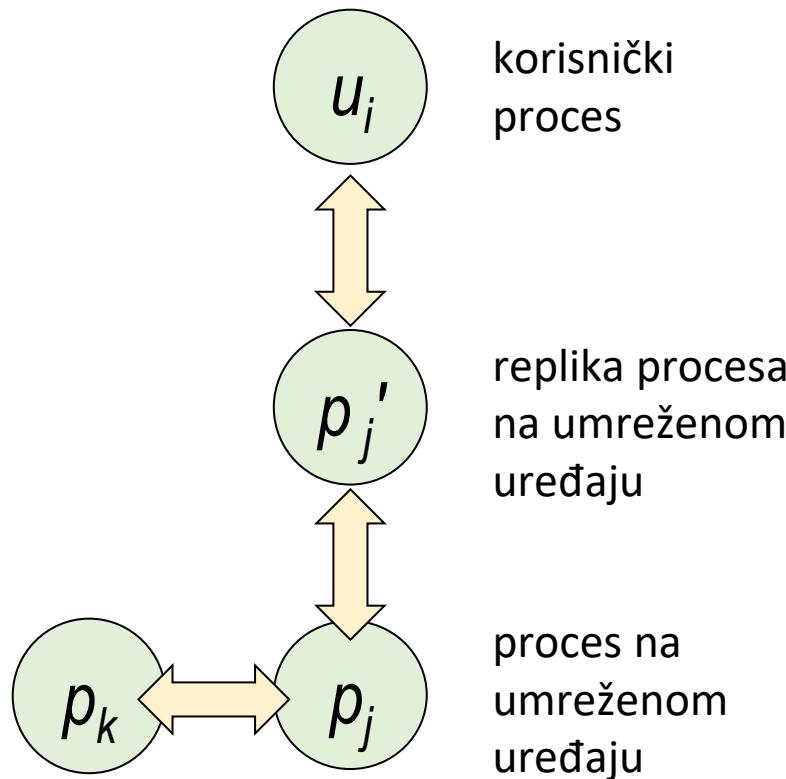
Vizija IoT-a prema *Web of Things*



- Raspodijeljeni sustav vođen događajima, modelira se I/O automatom
 - $u_i \in U$: U je konačni skup korisnika
 - $p_j \in P$: P je konačni skup uređaja
 - mogući događaji: *sense*, *actuate*, *send reading*
 - *send reading* je uvjetni događaj, posljedica *sense*

Programske platforme za IoT

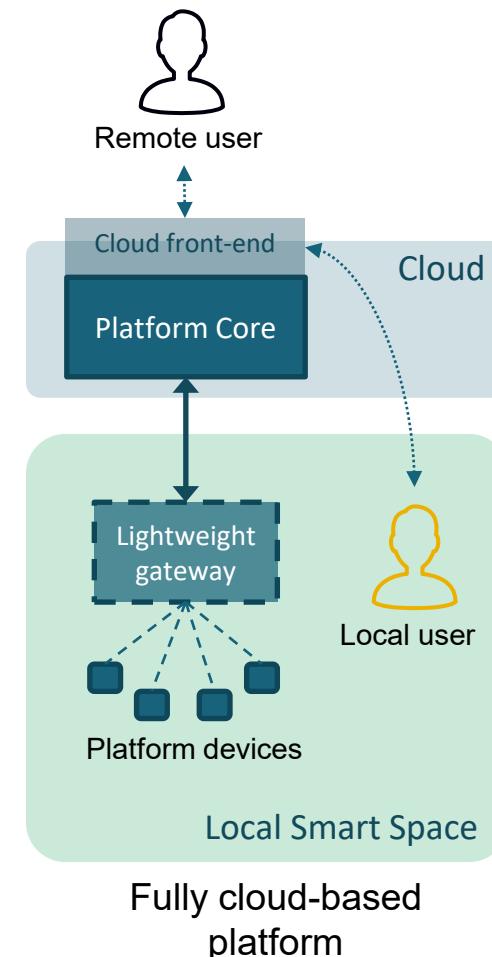
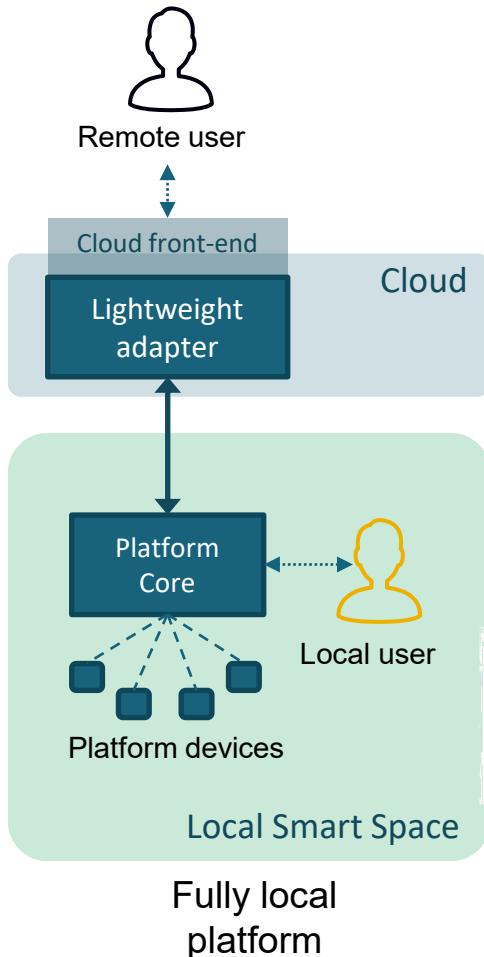
Proširen model IoT-sustava



Virtualni entitet predstavlja stvarni uređaj

- programska platforma održava metapodatke o uređajima
- pohranjuje senzorska očitanja, stanja aktuatora, obrađuje podatke

Vrste programskih platformi

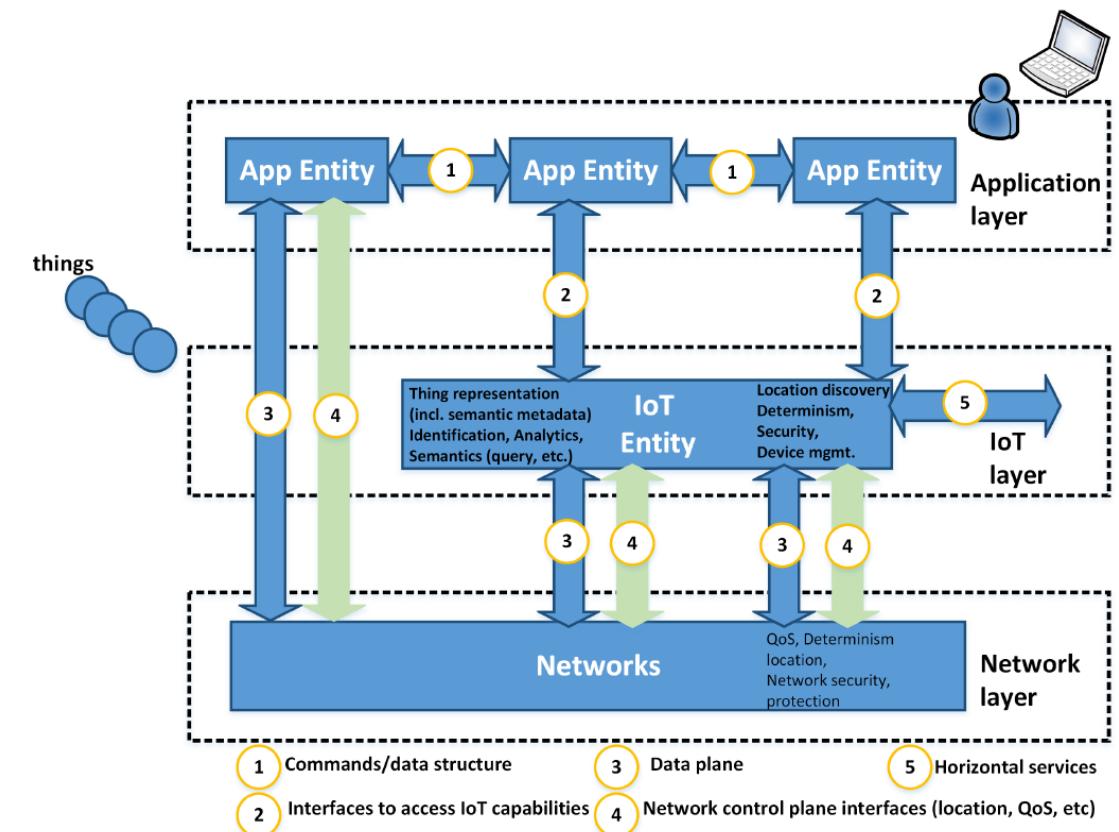


Referentne arhitekture (1/2)

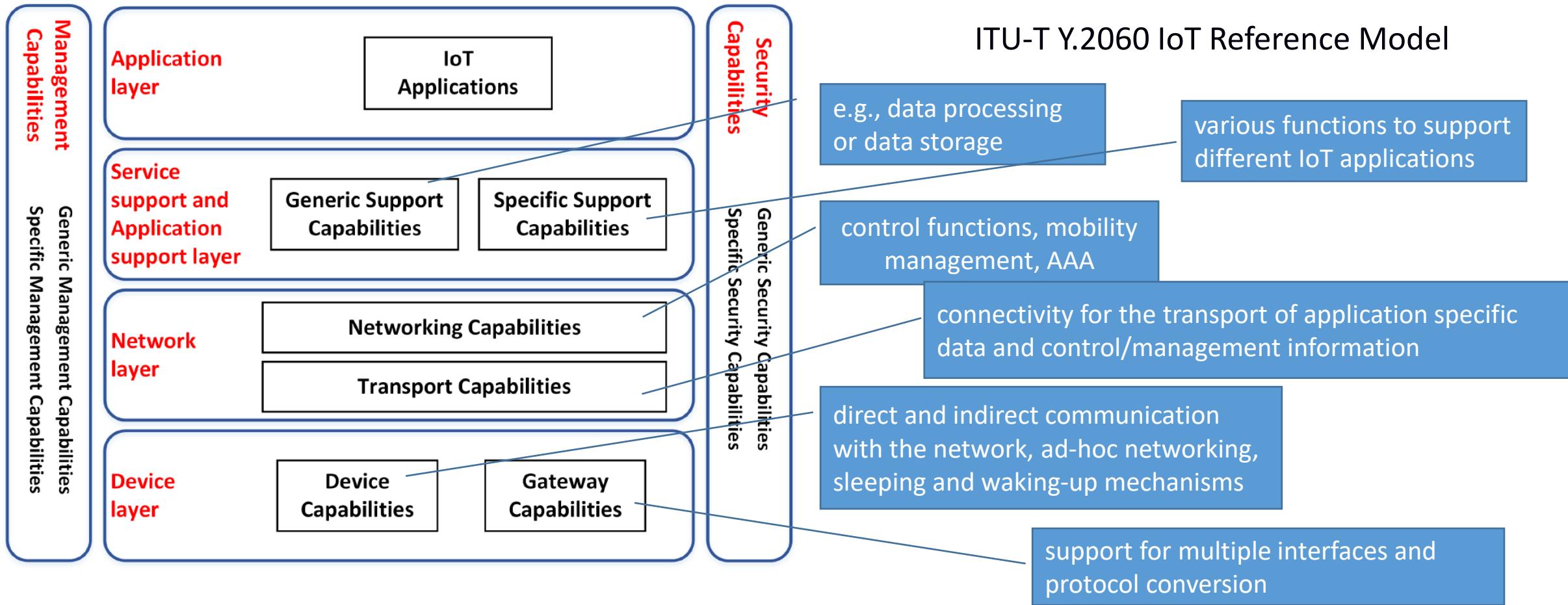
AIOTI HLA functional model

Konzorcij: Alliance for Internet of Things Innovation (AIOTI)

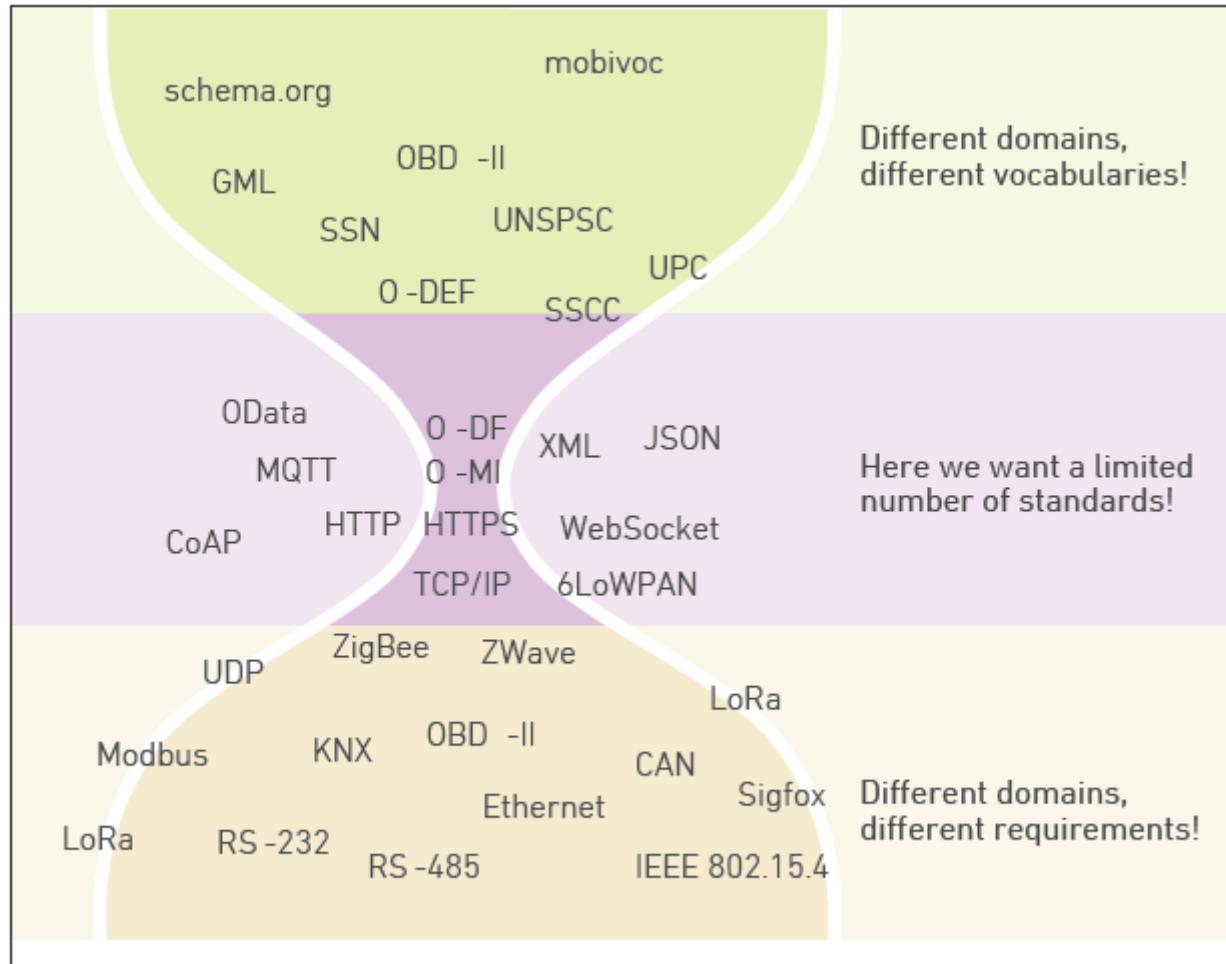
High Level Architecture (HLA)



Referentne arhitekture (2/2)



Različiti standardi i standardizacijska tijela



Web of Things at W3C



AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION



Izvor: IoT-EPI whitepaper, Advancing IoT Platforms Interoperability, 2018.

Izazovi IoT-a (1/2)

- Heterogeni uređaji i izvorni podataka, različiti protokoli
 - potrebno je osigurati interoperabilnost, uniforman pristup svim podacima
- Kontinuirano se generira velika količina podataka (*Big Data*) s obzirom na veliki broj izvora podataka
 - potreba za skalabilnom obradom i filtriranjem podataka u stvarnom vremenu
- **Veliki broj uređaja** koje je potrebno održavati
 - omogućiti pronalaženje uređaja, jednostavno povezivanje novih uređaja na Internet i samokonfiguracija stvari u "pametne okoline"
- **Sigurnost i privatnost**
 - veliki izazov za komercijalna rješenja, sigurnosni problemi u fizičkoj domeni (potencijalno mogu ugroziti ljudski život)
- Implementacija različitih **poslovnih modela**, **modeli naplate**
 - u inicijalnoj fazi, više na nivou ideje nego implementacije

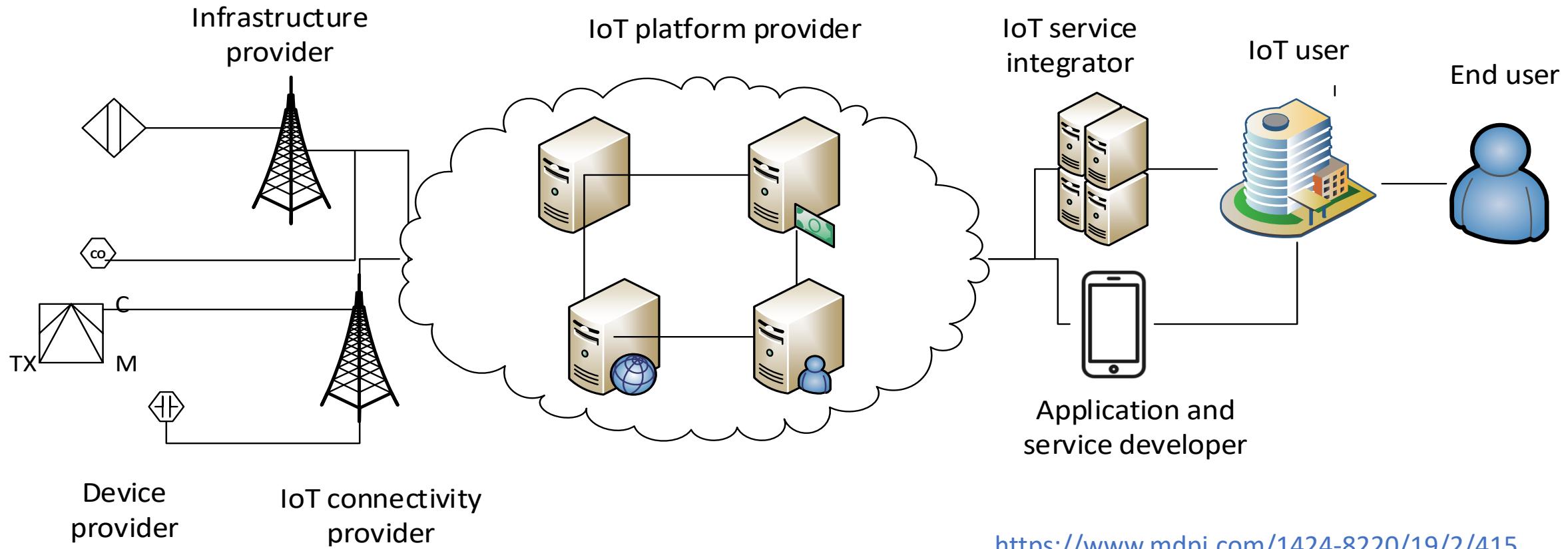
Izazovi IoT-a (2/2)

- Dinamične i prilagodljive aplikacije u skladu s kontekstom korisnika
- Fragmentacija tržišta
 - nova mobilna aplikacija za svaku umreženu stvar ili pametnu okolinu
- Integracija različitih vertikalnih rješenja u jedinstvenu IoT platformu
 - danas su na raspolaganju pretežno izolirana rješenja jednog ponuđača usluge u području IoT koji postavlja i integrira infrastrukturu u „pametnoj okolini” i nudi korisniku mobilne aplikacije za tu okolinu

Otvorena pitanja

- **Sigurnost**
 - Symantec 2018 Internet Security Threat Report (ISTR): broj napada na IoT uređaje je porastao 600 puta u 2017. u odnosu na 2016.
- **Privatnost**
 - Povećan je rizik povrede privatnosti i gubitka osobnih podataka, korisnici sve više postaju svjesni vrijednosti osobnih podataka te žele kontrolirati tko koristi njihove podatke (*podatkovni suverenitet*)
- **Skalabilnost**
 - Neće biti moguća bez interoperabilnih programskih rješenja
- **Decentralizacija**
 - Povjerenje (*trust*) postaje ključno za korisnike, trend primjene računalnih resursa „na rubu mreže“ i tehnologije blok-lanca

Lanac vrijednosti za IoT

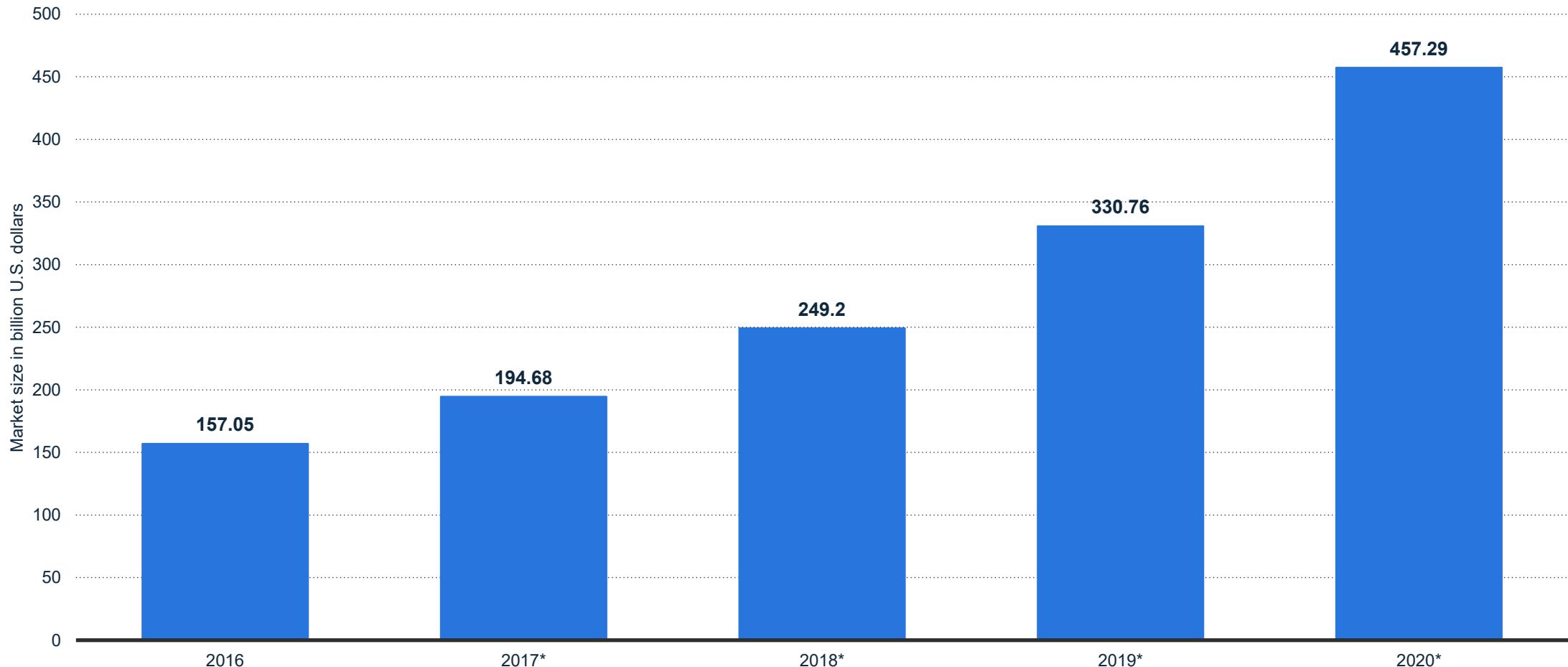


<https://www.mdpi.com/1424-8220/19/2/415>

Tržišni potencijal

Size of the IoT market worldwide from 2016 to 2020 (in billion U.S. dollars)

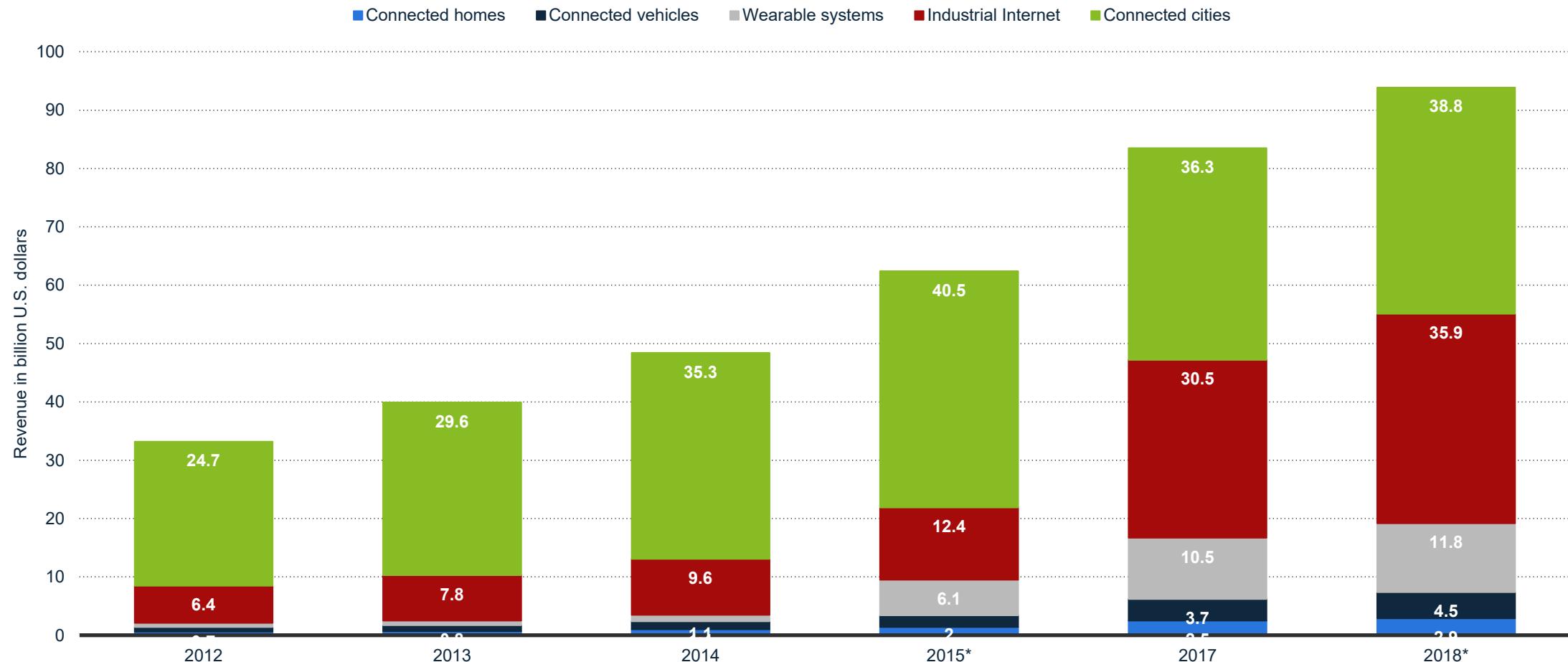
Global IoT market size 2016-2020



Izvor: Statista

Revenue of Internet of Things subsystems worldwide from 2012 to 2018 (in billion U.S. dollars)

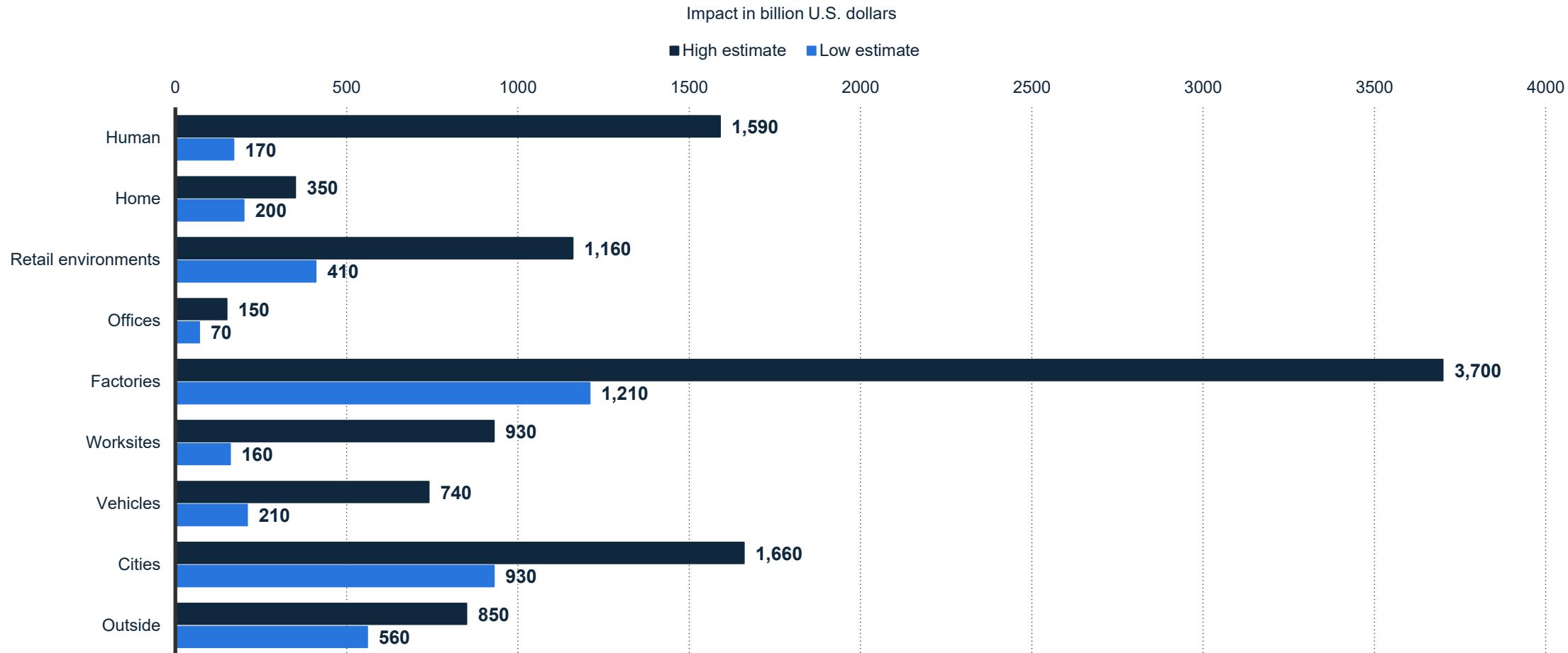
Internet of Things subsystems revenue worldwide 2012-2018



Izvor: Statista

Forecast economic impact of the Internet of Things (IoT) in 2025 (in billion U.S. dollars)

IoT economic impact forecast 2025, by sector



Izvor: Statista

Laboratorij za Internet stvari

<http://www.iot.fer.hr/>



Projekti

[IoT-polje: Ekosustav umreženih uređaja i usluga za Internet stvari s primjenom u poljoprivredi](#)

istraživački projekt financiran sredstvima ESIF

Suradne institucije: FERIT Osijek i Poljoprivredni institut Osijek

voditelj: prof. dr. sc. Ivana Podnar Žarko

(03/2020. – 02/2023.)

[Pametne usluge usmjerenе čovjeku u interoperabilnim i decentraliziranim okolinama Interneta stvari \(IoT4us\)](#)

istraživački projekt HRZZ broj 1986

voditelj: prof. dr. sc. Ivana Podnar Žarko

(2020.-2023.)

Razvoj agrometeorološke platforme i mreže IoT uređaja tvrtke Pinova d.o.o., istraživački projekt IRI II

voditelj: prof. dr. sc. Mario Kušek

(09/2020. – 08/2023.)

Novi projekt: Horizon Europe



AIoTwin
Twinning action for spreading excellence in Artificial Intelligence of Things

Trajanje: 01/2023-12/2025

No.	Participant Logo	Participant organisation name	Short Name	Country
1 (CO)	 <small>UNIVERSITY OF ZAGREB Faculty of Electrical Engineering and Computing</small>	University of Zagreb Faculty of Electrical Engineering and Computing	UNIZG- FER	Croatia
2		RISE Research Institutes of Sweden AB	RISE	Sweden
3	 TECHNISCHE UNIVERSITÄT WIEN	Technische Universität Wien	TUW	Austria
4	 Technische Universität Berlin	Technische Universität Berlin	TUB	Germany





SVEUČILIŠTE U ZAGREBU



Fakultet
elektrotehnike i
računarstva

**Diplomski studij
Računarstvo**

Znanost o mrežama

Programsko inženjerstvo i informacijski
sistemi

Računalno inženjerstvo

Informacijska i komunikacijska tehnologija

Automatika i robotika

Informacijsko i komunikacijsko inženjerstvo

Elektrotehnika i informacijska tehnologija

Audiotehnologije i elektroakustika

Elektroenergetika

(Izborni predmet profila)

Internet stvari

**2. Stvari i uređaji u IoT okruženju
(fizički sloj): senzori, aktuatori, prilaz
(gateway), komunikacija M2M**

Ak. god. 2022./2023.



Sadržaj

- Internet stvari (engl. *Internet of Things*, IoT)
- Sloj uređaja
- Sloj podatkovne poveznice: M2M-komunikacija
- Primjeri uređaja/prilaza za IoT

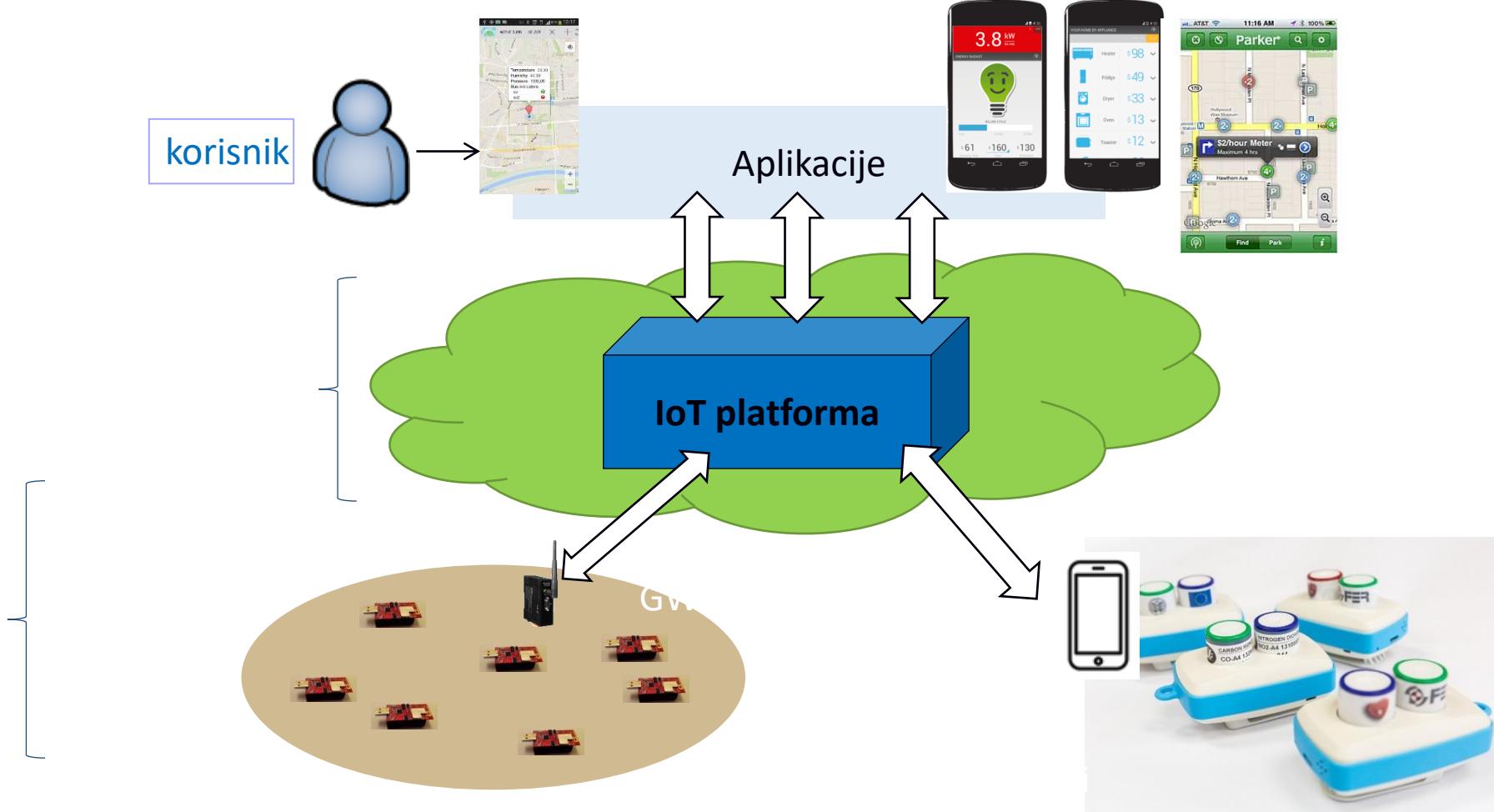
Internet stvari

Definicija*:

“A global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies” (ITU work on Internet of things, 2015).

„Globalna mrežna infrastruktura koja povezuje fizičke i virtualne objekte iskorištavajući dohvat podataka i komunikacijske mogućnosti. Ta infrastruktura uključuje postojeći i nastajući Internet i razvoj mreža. Omogućit će specifičnu identifikaciju objekata, senzore i povezivanje kao osnovu za razvoj neovisnih kooperativnih usluga i aplikacija. Sve će biti obilježeno visokim stupnjem samostalnog prikupljanja podataka, prijenosa događaja, mrežnog povezivanja i međudjelovanja.“ (CASAGRAS, EU Framework 7 Project “Coordination And Support Action for Global RFID-related Activities and Standardisation”, 2009.)

Pojednostavljena arhitektura Interneta stvari



IoT ekosustav

- (Pametni) uređaji – „stvari”: senzori i aktuatori
- Mrežna infrastruktura temeljena na protokolu IP:
 - Nepokretne mreže (xDSL, optika)
 - Pokretne mreže (2G, 3G, 4G, 5G) – NB-IoT, LTE-M
 - Bežične mreže – WLAN, LoRa/LoRaWAN
 - Osobne mreže – Bluetooth, 6LowPAN
- (Horizontalne) platforme za ostvarivanje usluga
- Povezane tehnologije
 - Računarstvo u oblaku i magli
 - Velika količina podataka
- Standardizacija i interoperabilnost imaju ključnu ulogu!

Sadržaj

- Internet stvari (engl. *Internet of Things*, IoT)
- Sloj uređaja
- Sloj podatkovne poveznice: M2M-komunikacija
- Primjeri uređaja/prilaza za IoT

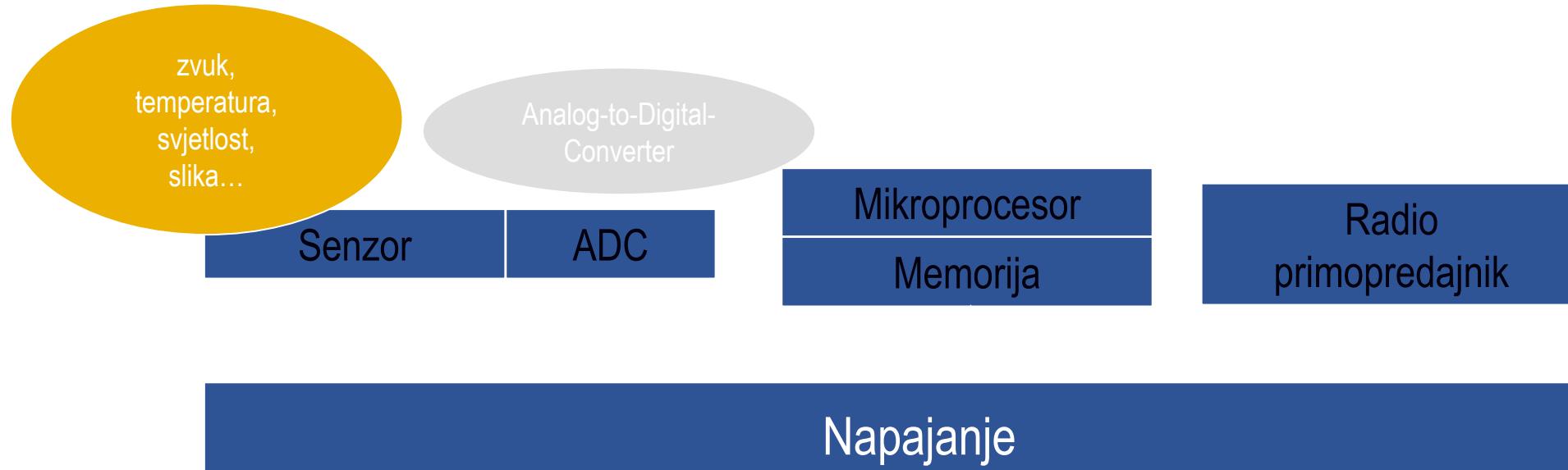
IoT-uređaj (senzorski čvor)

remote sensor, mote, smart dust

- uređaj za opažanje fenomena iz okoline, malih je dimenzija, troši мало energije (baterija), te posjeduje ograničene resurse
- primjena: mjeri atmosferske promjene, temperaturu, tlak, svjetlost, vibracije, ubrzanje, opaža zvuk/sliku (mikrofon, kamera)
- podatke šalje bežično do sljedećeg senzora ili do usmjeritelja (engl. gateway, GW) koji je povezan na Internet, nastaje bežična senzorska mreža (engl. Wireless Sensor Network, WSN)



Komponente IoT-uređaja



- sastoji se od komponenti za opažanje i mjerjenje fenomena iz okoline, procesora i memorije te komponente za komunikaciju
- ograničeno komunikacijsko područje pokrivanja zbog ograničenog napajanja

Aktuatori

actuator

- uređaj koji djeluje na okolinu, izvodi određenu akciju u okolini
- u kombinaciji sa senzorima na temelju očitanja iz okoline djeluju na okolinu

stvar – (pametni) uređaj – IoT-uređaj

- procesorska jedinica
- senzor i/ili aktuator
- komunikacijska jedinica
- napajanje

Obilježja hardvera

Zahtjevi

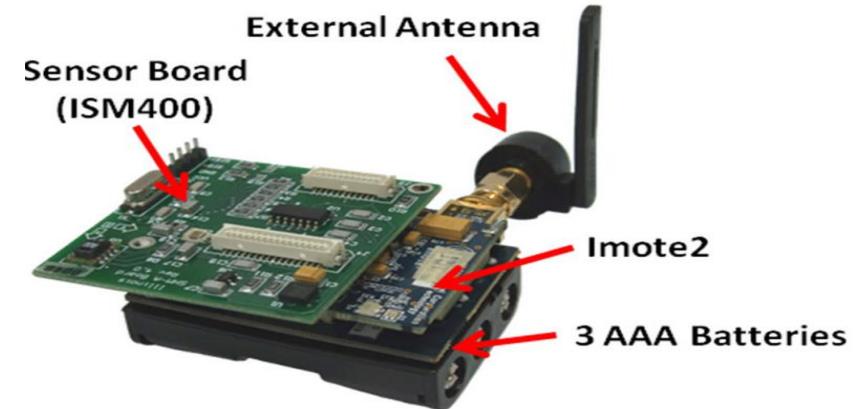
- izrazito male dimenzije
- mala potrošnja energije
- niska cijena
- umrežavanje na načelu samoorganizacije
 - najčešća uporaba u područjima bez postojeće mrežne infrastrukture
 - omogućiti umrežavanju uz slučajan raspored senzora na nekom zemljopisnom području
 - umrežavanje “pokretnih senzora”
 - veliki broj veza

IoT-uređaj ima izrazito ograničene resurse

- napajanje: **baterija** (najčešće), solarne čelije, vibracija, itd.
- **mikroprocesor**: samo osnovna procesorska svojstva radi niske potrošnje energije, ograničenih dimenzija i niske cijene
- **memorija**: ograničena, može pohraniti samo mali dio detektiranih podataka
- područje pokrivanja **radio predajnika**: relativno malo, troši najviše energije (snaga signala opada s kvadratom udaljenosti)

Primjeri IoT-uređaja

- Pioniri: Mica2 (Crossbow), IntelMote2 ili iMote2 (Intel, Crossbow)



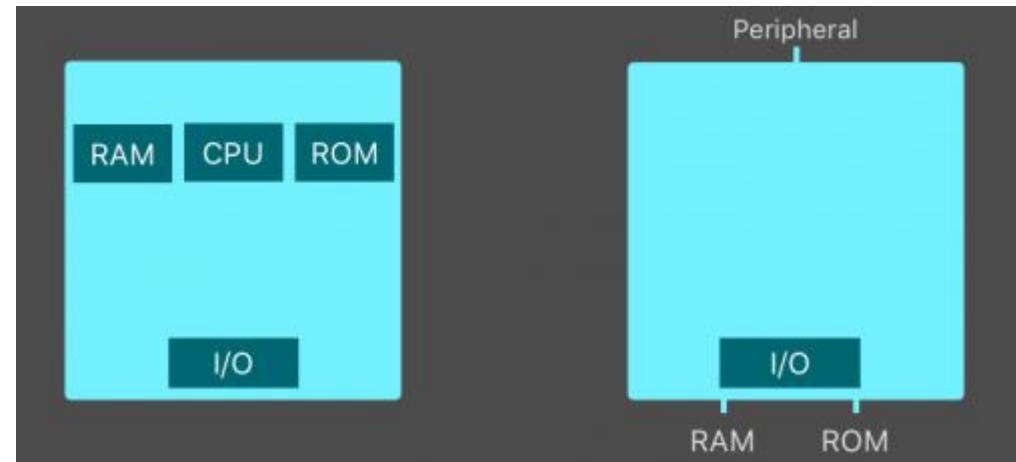
- WaspMote (Libelium):
Waspmote is Libelium's advanced mote for Wireless Sensor Networks.

<http://www.libelium.com/development/waspmote/documentation/waspmote-datasheet/>



Mikroprocesori i mikrokontroleri

- Mikrokontroler – na jednom čipu su integrirani:
 - Radna memorija (RAM)
 - Memorija iz koje se podaci samo čitaju (ROM)
 - Interna sabirnica za komunikaciju s drugim entitetima



Podjela mikrokontrolera

- Po bitovima
 - 8, 16, 32, 64
- Po arhitekturi - modeli
 - Von Neumann
 - Harvard
- Arhitektura
 - ARM
 - MIPS
 - x86

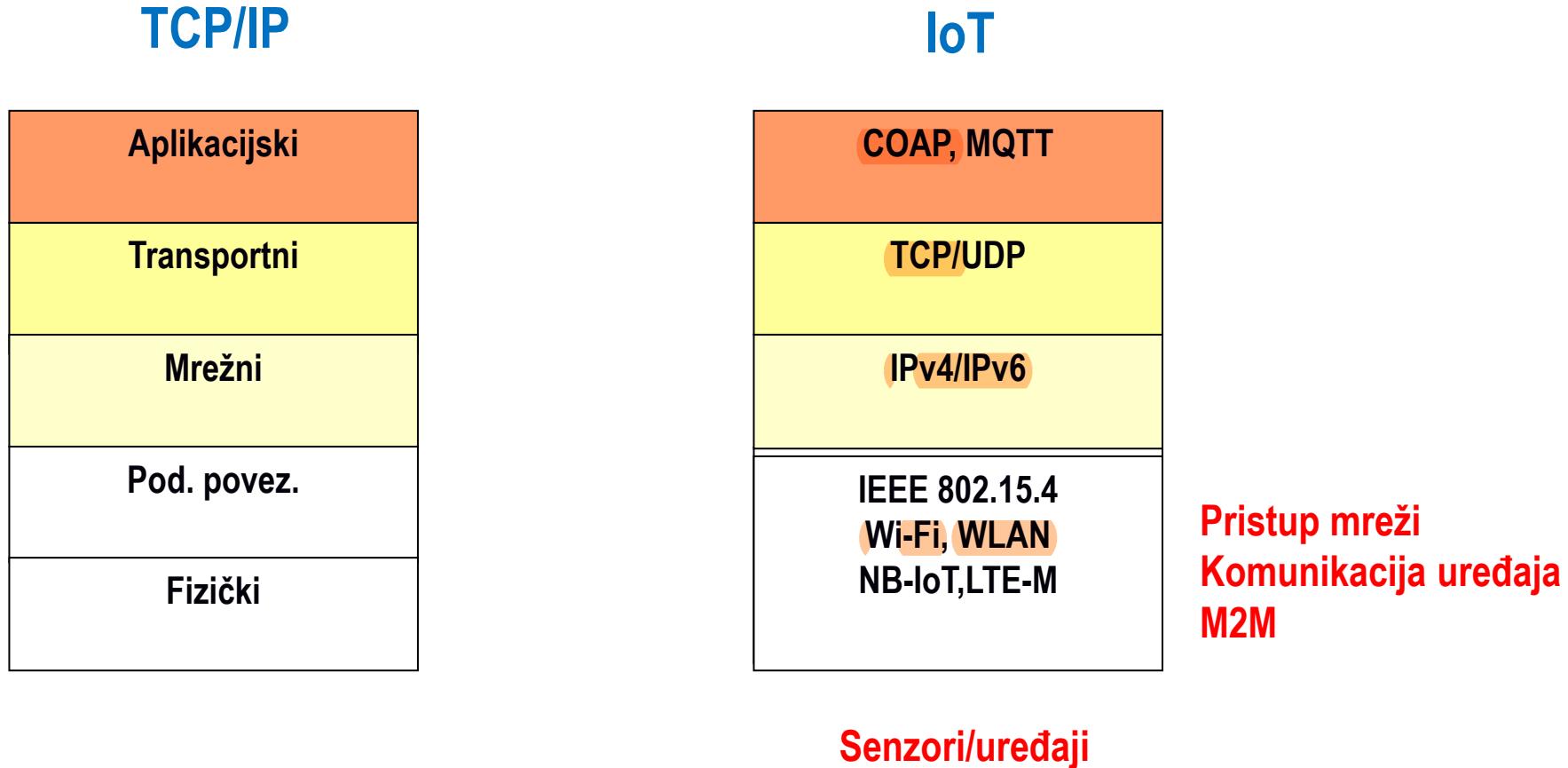
Bitna svojstva mikrokontrolera

- Procesorska snaga
- Memorija
- Potrošnja energije
- Brzo buđenje
- Komunikacijski moduli
- Sigurnost, enkripcija

Sadržaj

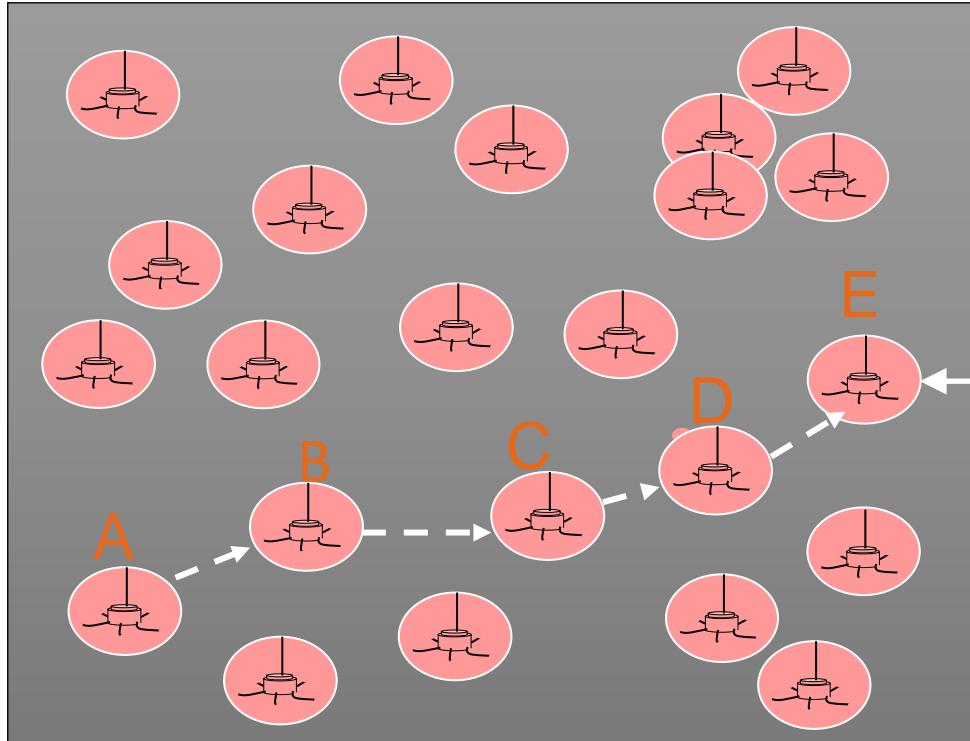
- Internet stvari (engl. *Internet of Things*, IoT)
- Sloj uređaja
- Sloj podatkovne poveznice: M2M-komunikacija
- Primjeri uređaja/prilaza za IoT

Protokolni složaj IoT

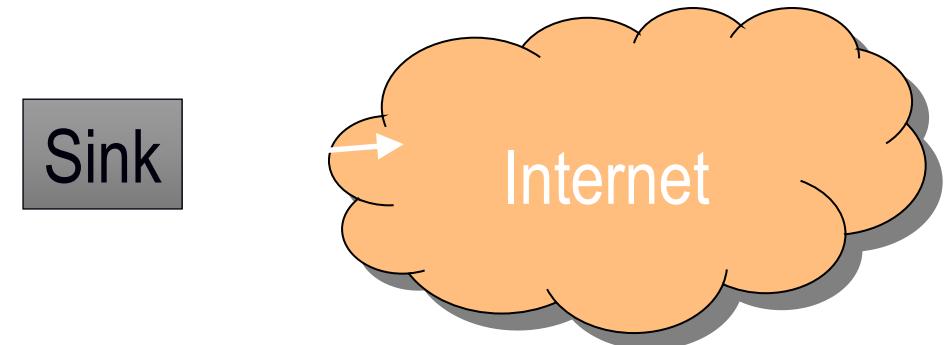


Bežična mreža senzora (WSN)

“preteča” današnjih rješenja za IoT



Mrežu senzora čini skup senzora na nekom zemljopisnom području koji međusobno surađuju.



Senzori detektirane podatke šalju do posebnog čvora (*sink*) – može imati vezu na Internet

Razlike u odnosu na ad hoc mreže

- broj senzora u mreži je znatno veći nego broj čvorova u adhoc mreži
- senzori se postavljaju gusto zbog komunikacijskih ograničenja
- senzori su skloni ispadima, česta izmjena baterija
- topologija mreže senzora je stabilnija
- senzori često nemaju globalni identifikator
- vrlo ograničeni resursi

Različite vrste mreža senzora

- Kopnena mreža senzora
 - 100 do 1000 jeftinih senzora raspoređenih slučajno ili planski na ograničenom zemljopisnom području
- Podzemna mreža senzora
 - nešto skuplji senzori se ugrađuju u zemlju, stijene, glečere, itd.
 - planski raspored senzora, sink je na površini
- Podvodna mreža senzora
 - vrlo skupi senzori, prenose ih često podvodna vozila, ograničena bežična komunikacija pod vodom
- Višemedijska mreža senzora
 - senzori s kamerama i mikrofonima, raspoređuju se planski
- Pokretna mreža senzora
 - senzori na pokretnim telefonima, robotima, vozilima, u interakciji su sa statičkim senzorima u okolini

Izazovi

- Raspored senzora na zemljopisnom području
 - planski ili slučajan (ovisi o primjeni)
 - utječe na potrošnju energije koja je ključna za neke aplikacije
 - često je nemoguće sve senzore postaviti u blizinu čvora sink
- Strategije slanja podataka sa senzora prema sinku (ovisi o primjeni!)
 - kontinuirana periodička isporuka
 - slanje na temelju opaženog značajnog događaja
 - slanje odgovora na eksplicitni upit
- Senzori mogu generirati redundantne podatke
 - “čišćenje” i agregacija podataka u samoj mreži tijekom prijenosa (eliminacija duplikata, min, max, average...)

M2M

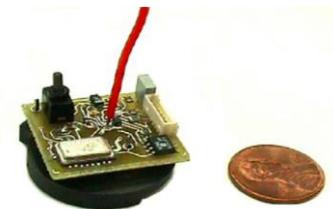
Machine-to-Machine, M2M

Machine Type Communication, MTC

- Sustavi temeljeni na komunikaciji uređaja
 - bez, ili samo s ograničenom intervencijom čovjeka
 - jednostavni i/ili pametni (engl. *smart*) uređaji
 - komunikacija se ostvaruje različitim mrežnim tehnologijama

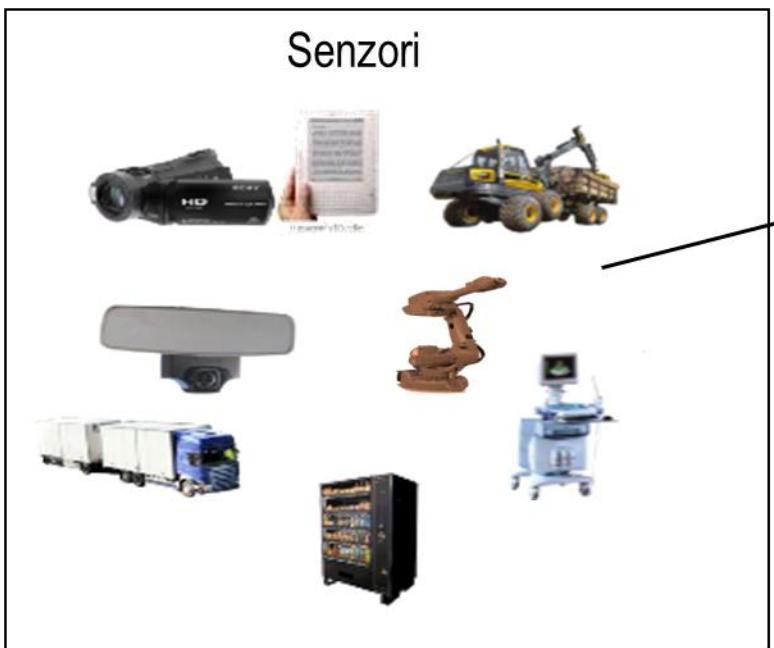
Machine-to-Machine

- Machine-to-Machine
 - senzori (mjerjenje protoka vode, temperature,...), pametna osjetila
 - aktuatori, ugrađeni procesori,...
- Machine-to-Machine
 - mreža koja omogućava komunikaciju krajnjih uređaja
 - pristupna mreža (bežična, pokretna, žična)
 - jezgrena mreža
 - pristupni uređaj (engl. *gateway*)
- Machine-to-Machine
 - računalni sustav koji upravlja drugim uređajima
 - računala i pokretni uređaji koji prikazuju informacije

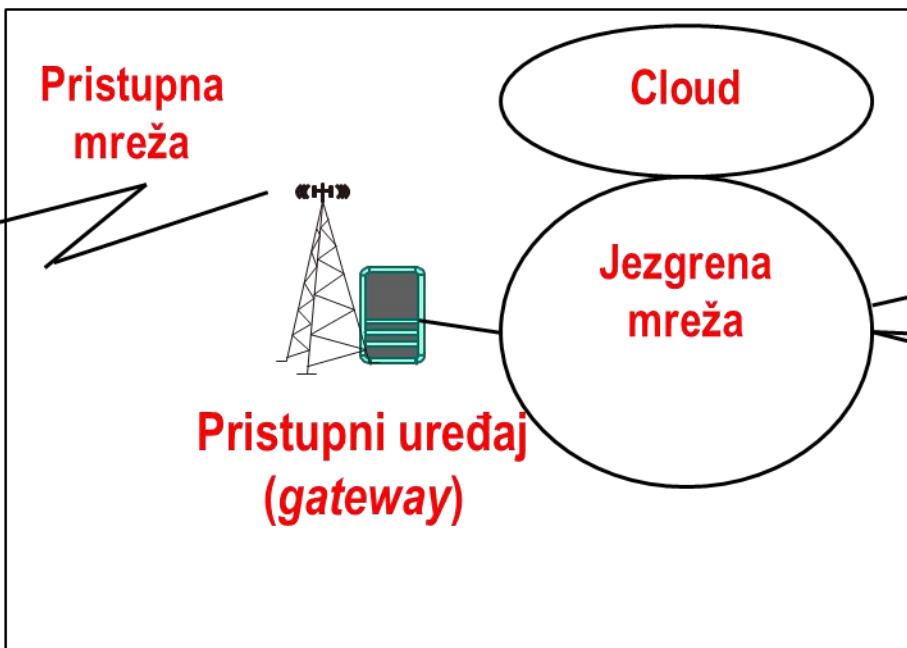


M2M

Bežična, pokretna, žična



Bežična, pokretna, žična



Uslužna domena
Aplikacija



Uredaji

Mreža senzora

M

Mreža

2

Uredaji

M

Uređaji

- IoT-uređaji

- spajaju senzore i aktuatore
- Mogu biti povezani na
 - bežičnu mrežu
 - kapilarna mreža/kratki domet – NFC, RFID (cm)
 - BlueTooth Low Energy (BLE) – IEEE 802.15.1, 6LoWPAN, LR-WPAN (XBee, ZigBee) - IEEE 802.15.4 (m)
 - WLAN, WiFi - IEEE 802.11, (m)
 - WiMAX – IEE 802.16, LoRaWAN, Sigfox (km)
 - pokretnu mrežu (km)
 - 2G/3G (EC-GSM-IoT)
 - 4G/5G (LTE-M, NB-IoT)
 - žičnu mrežu
 - fiksna mreža, xDSL, parica, optika (FTTH)

Mreža

- Jezgrena mreža
 - veza s korisnikom
 - internetska mreža
 - uslužne aplikacije
- Pristupni uređaj (engl. M2M gateway)
 - povezuje pristupnu i jezgrenu mrežu
 - NAT, sigurnost
 - (de)fragmentacija IP-paketa,...

NFC i RFID

- Near Field Communication

- 13.56 MHz
- 106-424 kbit/s
- domet do 10 cm
- koristi elektromagnetsku indukciju za komunikaciju
- aktivni i pasivni uređaji

- Radio-Frequency Identification

- radijski predajnik i prijamnik (tag)
- aktivni (imaju bateriju) i pasivni uređaji (indukcija)

Sadržaj predavanja

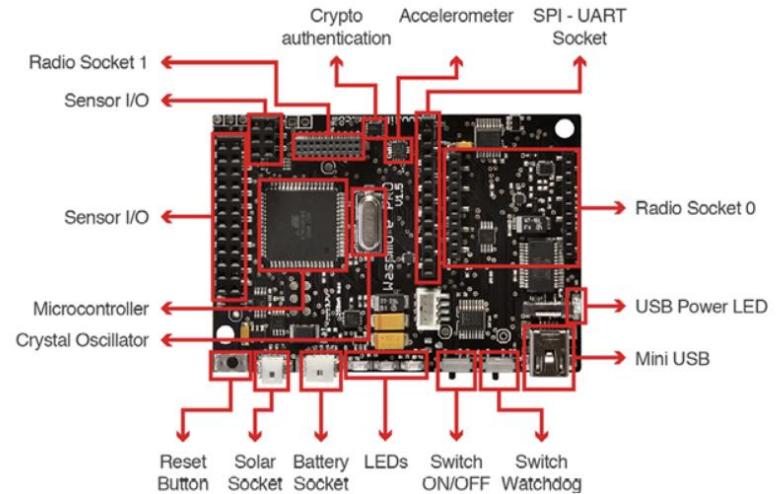
- Internet stvari (engl. *Internet of Things*, IoT)
- Sloj uređaja
- Sloj podatkovne poveznice: M2M-komunikacija
- Primjeri uređaja/prilaza za IoT

IoTLab@FER

- Wasp mote
- ESP32
- Pycom
- Raspberry Pi
- Strato Pi

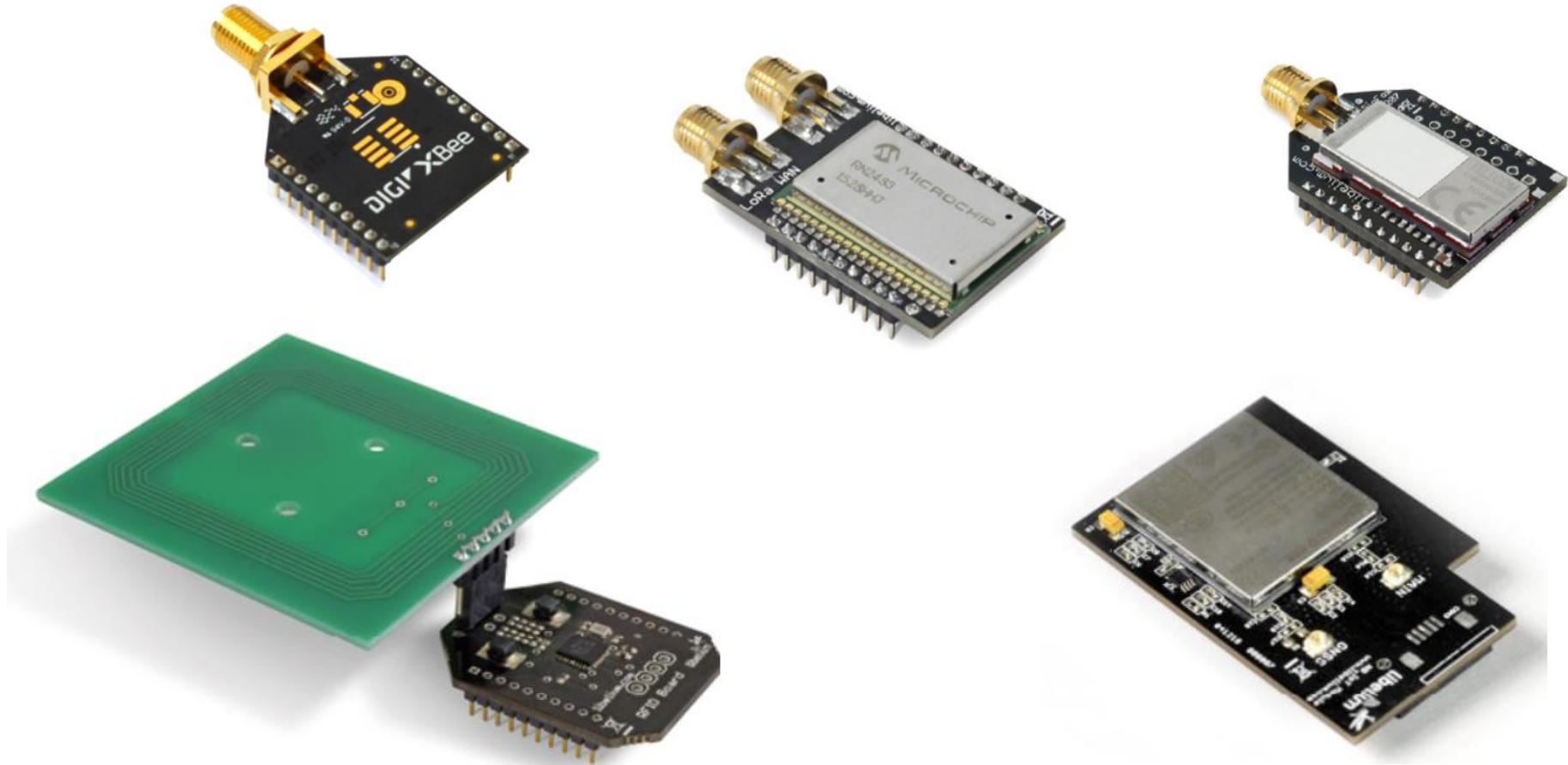
Libelium WaspMote

- Mikrokontroler ATmega1281
- Frekvencija: 14MHz
- SRAM (statička radna memorija): 8KB
- EEPROM (obrisiva programabilna stalna memorija): 4KB
- FLASH (stalna memorija – brisanje u blokovima): 128KB
- SD kartica: 2GB



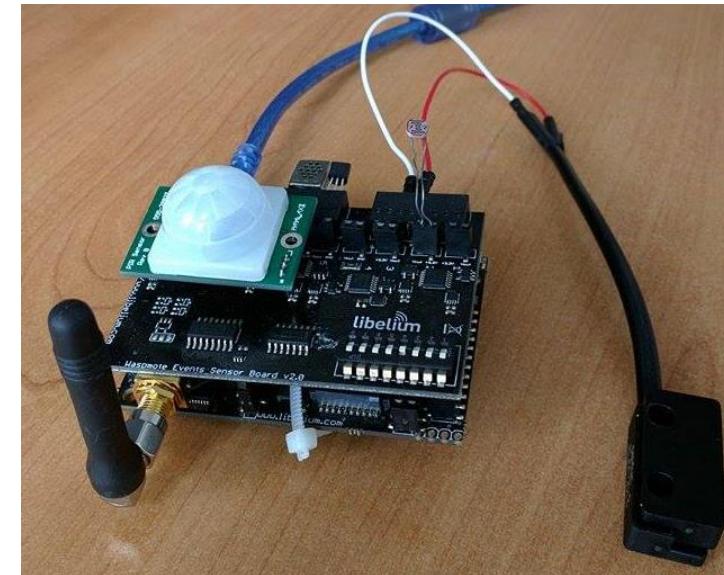
Komunikacijski moduli

- XBee
- Bluetooth
- WiFi
- NB-IoT
- LoRaWAN
- Sigfox
- RFID/NFC



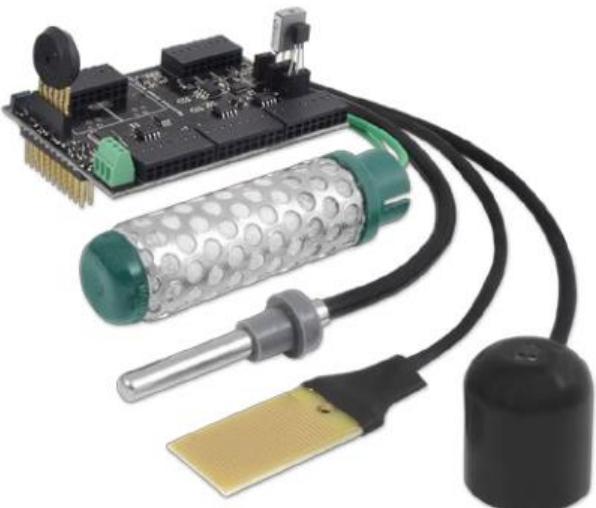
Senzorske pločice (engl. *sensor board*)

- Događaji (engl. *events*)
 - Senzor za pristutstvo
 - Temperatura
 - Protok vode
 - Magnetski senzori za vrata i prozore
- Pametni gradovi (engl. *smart cities*)
 - Kvaliteta zraka (plinovi, prašina)
 - Glasnoća
 - Detekcija pukotina u zgradama



Senzorske pločice (2)

- Poljoprivreda (engl. *agriculture*)
 - Vlažnost listova
 - Promjer plodova
 - Vlažnost tla
- Video kamera
 - Snimanje videa
 - Snimanje fotografija
 - Video-poziv



ESP32

- CPU: Xtensa dual-core 32-bitni LX6 mikroprocesor
 - RAM: 520 KB na mikroprocesoru + 16KB na RTC-u
 - ROM: 448 KB
 - vanjska memorija (flash): 4MB
-
- Sučelja: UART (*universal asynchronous receiver-transmitter*), SPI (*serial peripheral interface*), I2C (*inter-integrated circuit*), SD kartica
 - Komunikacijski moduli: WiFi, Bluetooth



pycom fipy

- Espressif ESP32 SoC
- CPU: Xtensa dual-core 32-bitni LX6 mikroprocesor
- RAM: 520 KB na mikroprocesoru + 16KB na RTC-u + 4MB eksterno
- vanjska memorija (flash): 8MB

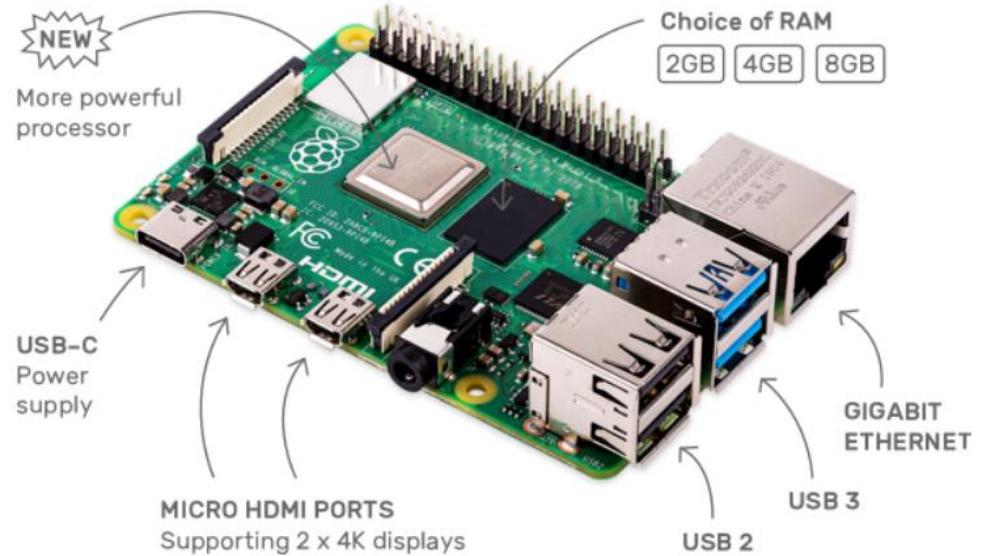


pycom fipy – komunikacijski moduli i senzori

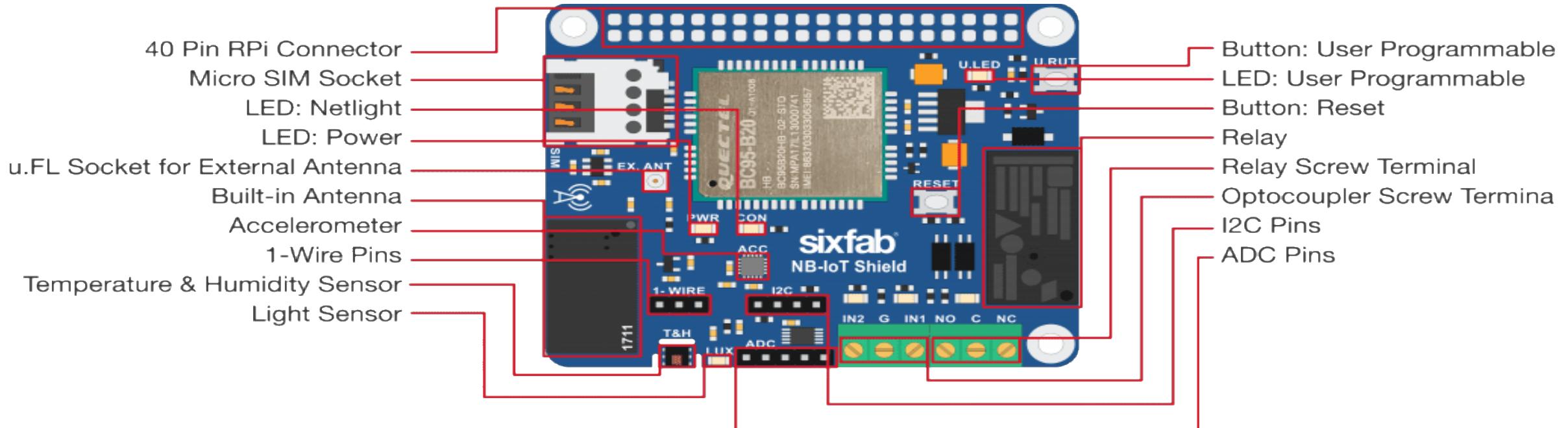
- LoRa
- Sigfox
- NB-IoT
- WiFi
- Bluetooth
- 22GPIO pina, sučelja: UART (*universal asynchronous receiver-transmitter*), SPI (*serial peripheral interface*), I2C (*inter-integrated circuit*), SD kartica

Raspberry Pi

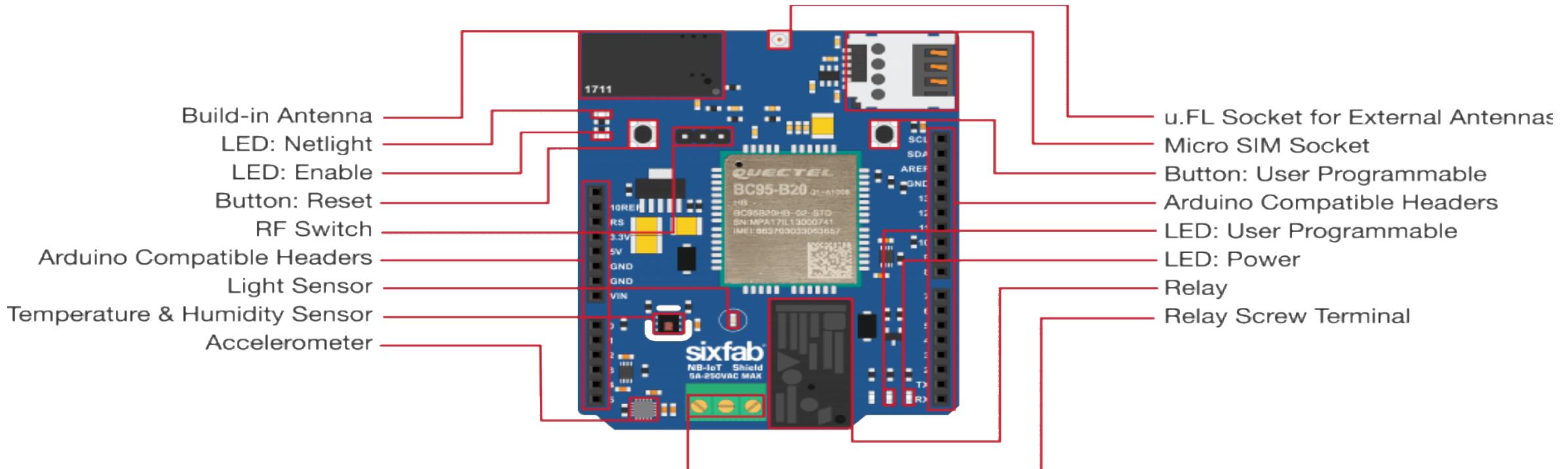
- CPU: Broadcom, quad-core 64-bitni ARM A72
- Frekvencija: 1.5 GHz
- RAM: 2/4/8 GB



Sixfab Raspberry Pi NB-IOT



Sixfab Arduino NB-IOT



Strato Pi

- Raspberry Pi za profesionalno i industrijsko okružje
- Stabilnije napajanje
- integrirano neprekidno napajanje (engl. *uninterruptible power supply*, UPS)
- Sadrži RTC (RPi ga nema)
- Podrška za serijsku komunikaciju (protokol RS-485) i komunikaciju preko sabirnice CAN (engl. *Controller Area Network*)



Literatura

1. C. Aggarwal, N. Ashish, and A. Sheth. [The Internet of Things: A Survey from The Data-Centric Perspective](#), Book Chapter in "Managing and Mining Sensor Data", Springer, 2013.
2. Charith Perera, Chi Harold Liu, Srimal Jayawardena. "[The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey](#)", IEEE Transactions On Emerging Topics In Computing 01/2015;
3. Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "[Wireless sensor network survey](#)," *Computer Networks*, Vol. 52, No. 12, pp. 2292-2330, August 2008.
4. Feng Wang; Jiangchuan Liu; , "[Networked Wireless Sensor Data Collection: Issues, Challenges, and Approaches](#)," *IEEE Communications Surveys & Tutorials*, vol.13, no.4, pp.673-687, Fourth Quarter 2011

Literatura

- J. Brown: "Machine-2-Machine, Internet of Things, Real World Internet", 2011.
- D. Boswarthick, O. Elloumi, O. Hersistent: "M2M Communications: A Systems Approach", Wiley, 2012.
- "M2M: Growth Opportunities for MNOs in developed Markets (Sample Pages)", Mobile Market Development Ltd., 2010.
- V. Galetić, I. Bojić, M. Kušek, G. Ježić, S. Dešić, D. Huljenić: "Basic principles of Machine-to-Machine communications and its impact on telecommunication industry" *MIPRO 2011*, pp. 380-385, 2011.
- "Machine to Machine Communications", <http://www.etsi.org/website/technologies/m2m.aspx>
- "M2M goes global: OneM2M", [http://open.actility.com/ node/104](http://open.actility.com/node/104), 2012.
- ETSI Technical Report 102 691: "Smart Metering Use Cases", v1.1.1, 2010.
- [oneM2M Use cases collection, Technical Report, 2013.
- "Machine to Machine Communications", <http://www.etsi.org/website/technologies/m2m.aspx>
- Katušić, D.; Ježić, G.; Marčev, A.; Vulas, R., Machine-to-Machine: Emerging Market and Consequences on Existing Regulatory Framework, Proceedings The 3rd Workshop on Electronic Communications Regulatory Challenges in the Electronic Communications Market, ConTEL 2013, 317-324, 2013.



SVEUČILIŠTE U ZAGREBU



**Diplomski studij
Računarstvo**

Znanost o mrežama

Programsko inženjerstvo i informacijski
sistemi

Računalno inženjerstvo

Informacijska i komunikacijska tehnologija

Automatika i robotika

Informacijsko i komunikacijsko inženjerstvo

Elektrotehnika i informacijska tehnologija

Audiotehnologije i elektroakustika

Elektroenergetika

(Izborni predmet profila)

Internet stvari

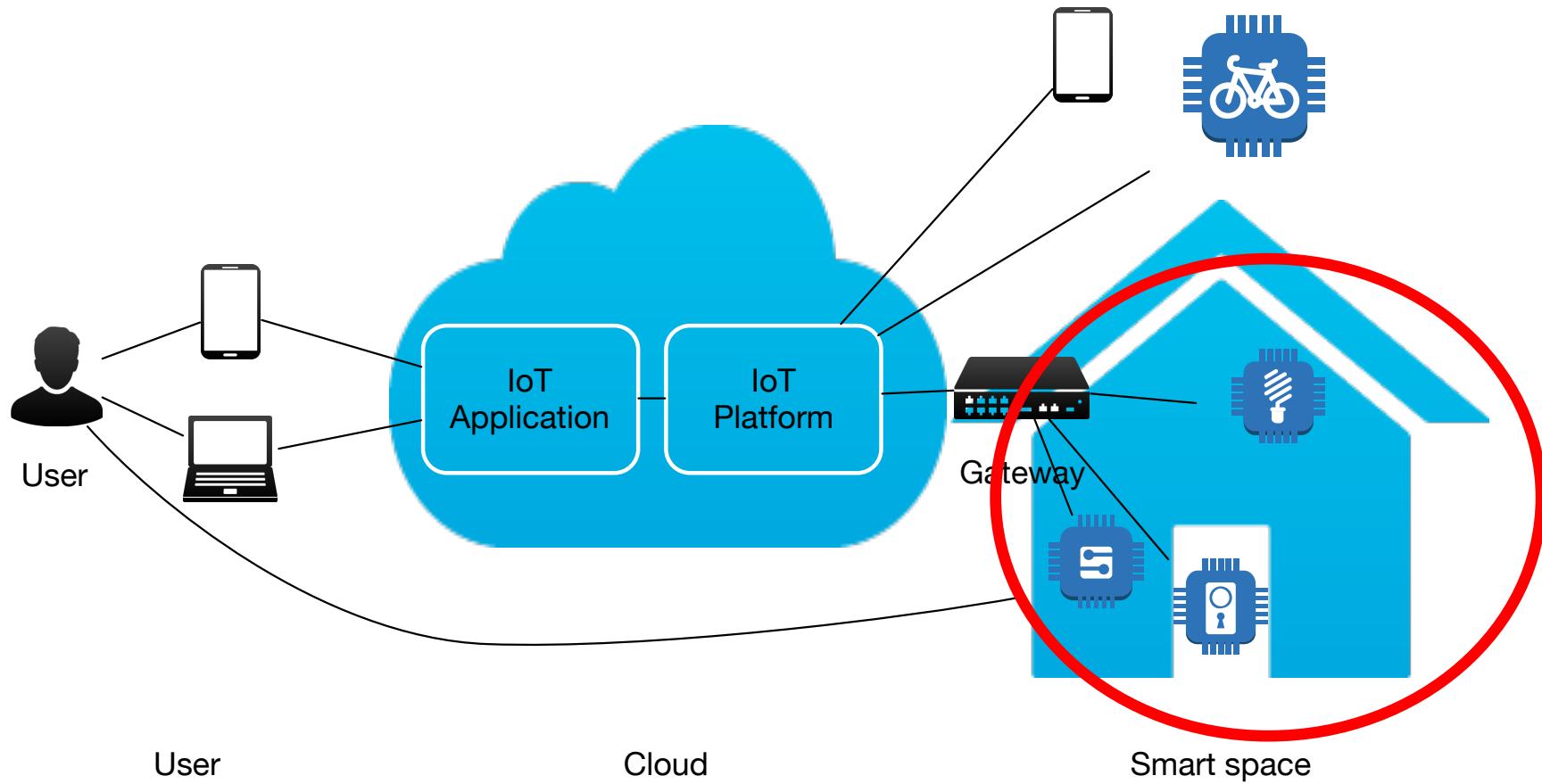
**3. Komunikacijski protokoli za
komunikaciju uređaja (sloj podatkovne
poveznice): IEEE 802.15.4, 802.11ah,
ZigBee, Z-Wave.**

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

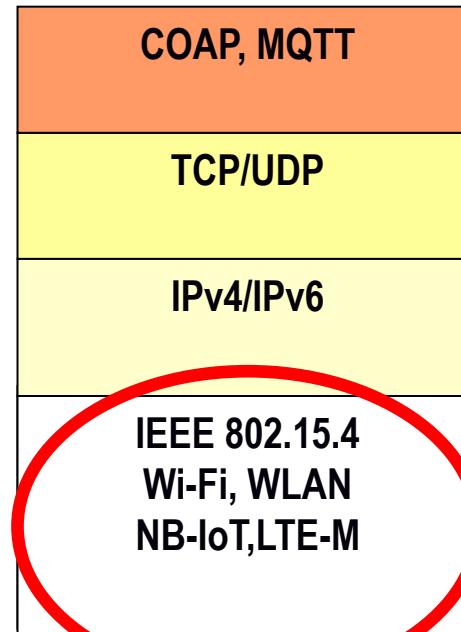


Protokolni složaj IoT-a

TCP/IP



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
E0	Ograničenje 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	Priklučeno na napajanje

Potrošnja energije – klasifikacija (2)

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

Ime	Strategija	Mogućnost komunikacije
P0	Normalno je isključeno	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 sklopolja (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)
Sinkronizacijsko zaglavlje 5 okteta		PHY zaglavlje 1 oktet	0-127 okteta

- Polja:
 - Preamble (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	Izvořište PAN ID	Izvořišna adresa	Sadržaj okvira	Frame Check Sequence
2 okt.	1 okt.		Adrese – 4-20 okt.			varijabilno	2 okt.
MAC zaglavje						MAC sadržaj	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 izbjegavanje sudara okvira – 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-bit
- 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 zaglavljje sigurnosti	Sadržaj okvira	Frame Check Sequence
2 okt.	1 okt.	Adrese – 4-20 okt.						0-14 okt
MAC zaglavljje						MAC sadržaj	MAC podnožje	

ZigBee



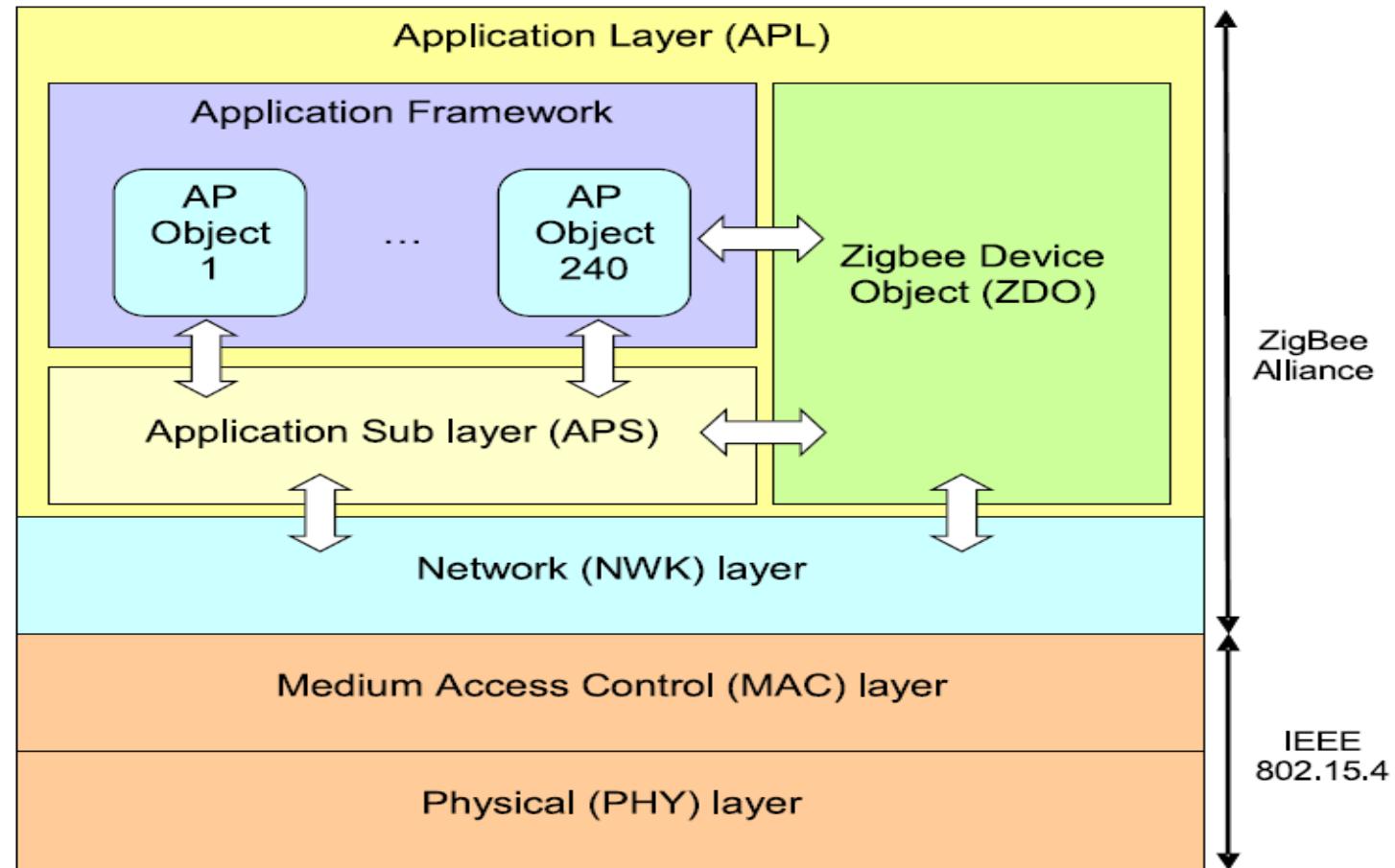
- Preko 300 kompanija je sudjelovalo u njegovoj standardizaciji u sklopu ZibBee Alliance
- Temelji se na standardu IEEE 802.15.4
- Namijenjen primjenama koje zahtjevaju malu brzinu veze, nisku potrošnju energije, malo kašnjenje, sigurnu komunikaciju (128-bit AES encryption)
- Čvorovi se u nekoliko milisekundi 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.

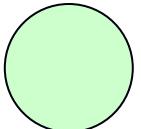
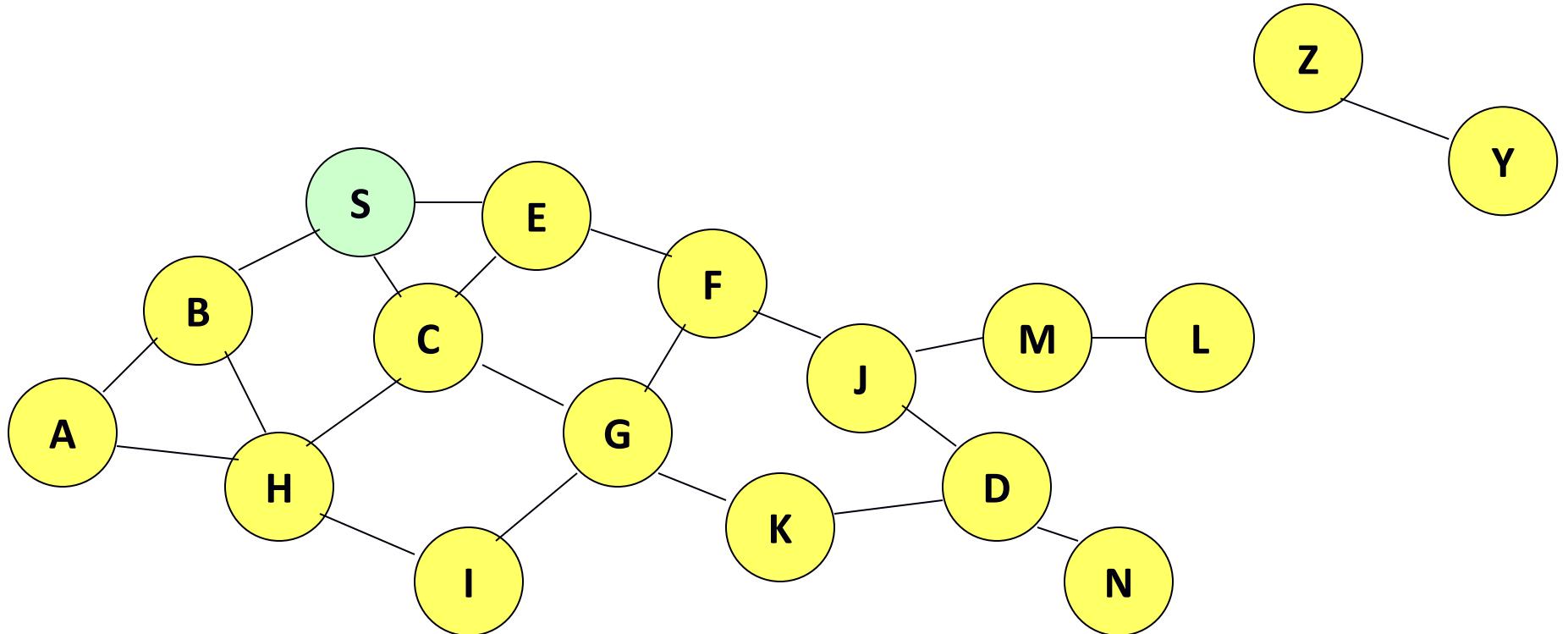
ZigBee – funkcije mrežnog sloja (NWK)

- 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

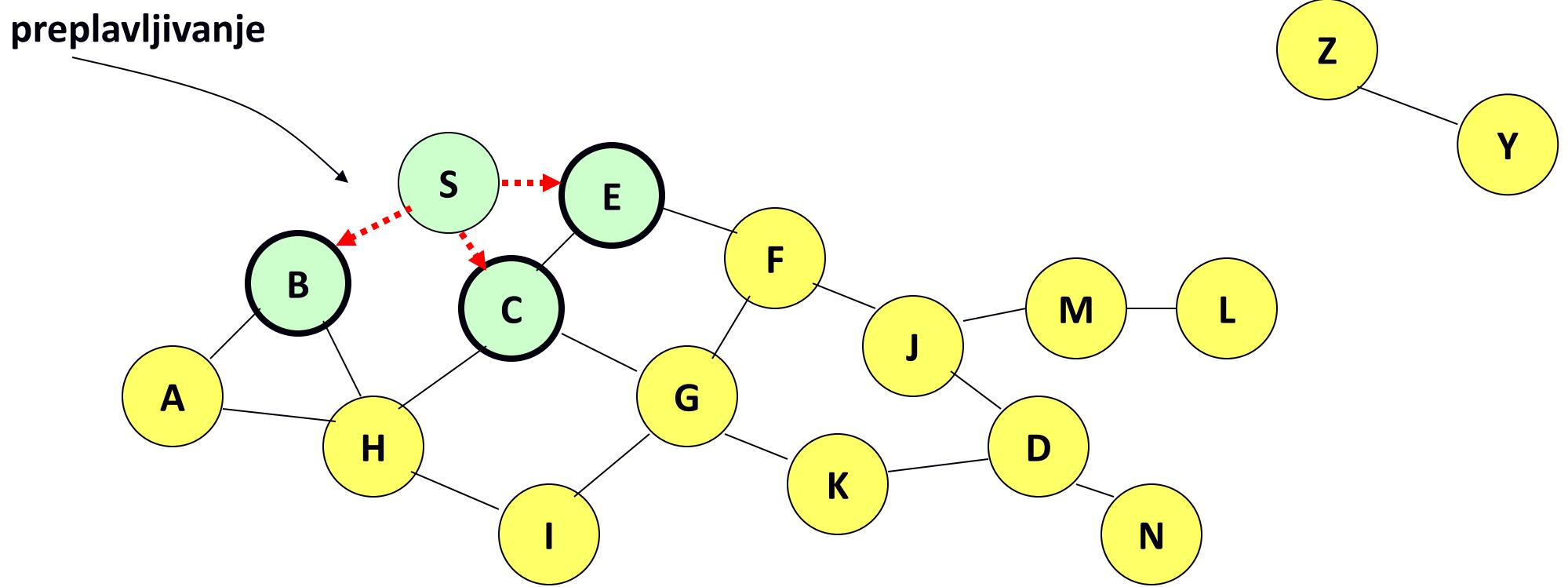
- *Ad Hoc On-Demand Distance Vector Routing* (AODV)
- održava tablice usmjeravanja na putu među čvorovima koji žele komunicirati
- preplavljanje porukama *route request* (RREQ) iz izvorišnog čvora S da bi se otkrio put do odredišta D
- čvor koji primi RREQ osvježava informaciju u tablici usmjeravanja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

AODV - *route request*

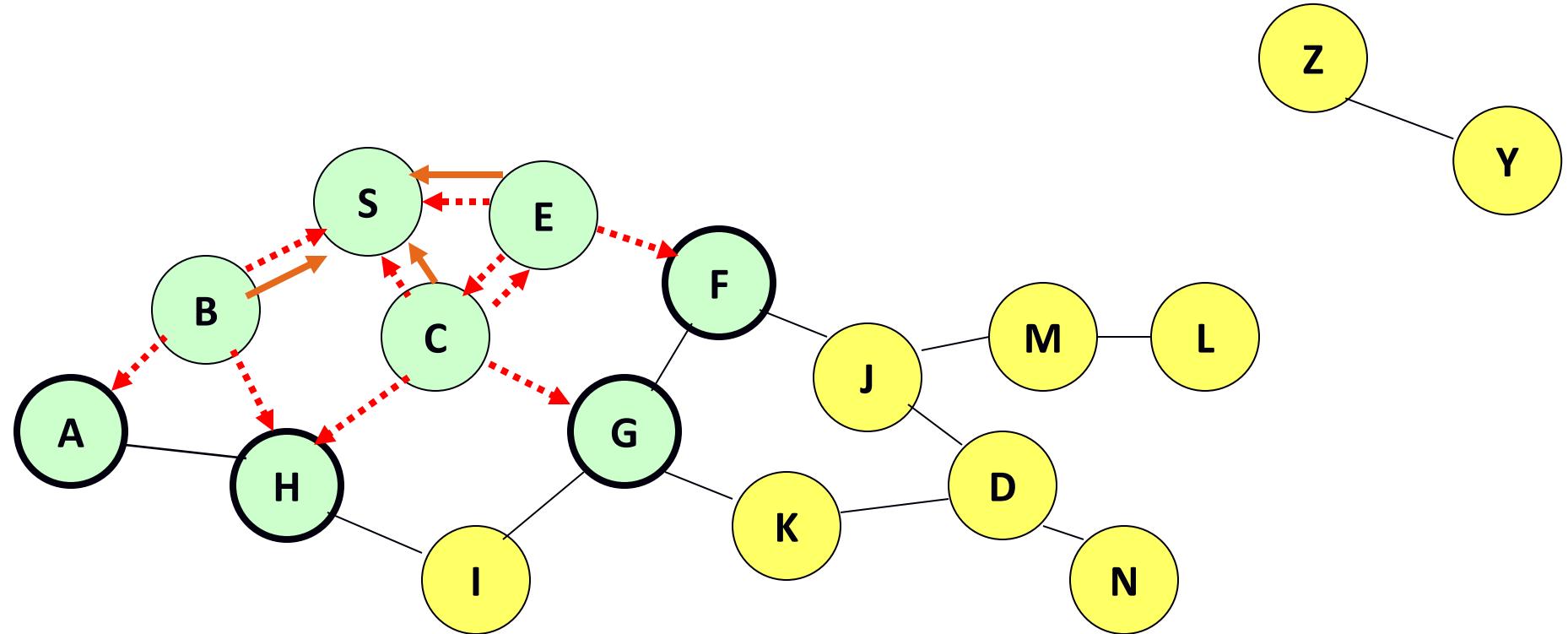


Oznaka čvora koji je primio RREQ za D od S

AODV - *route request*

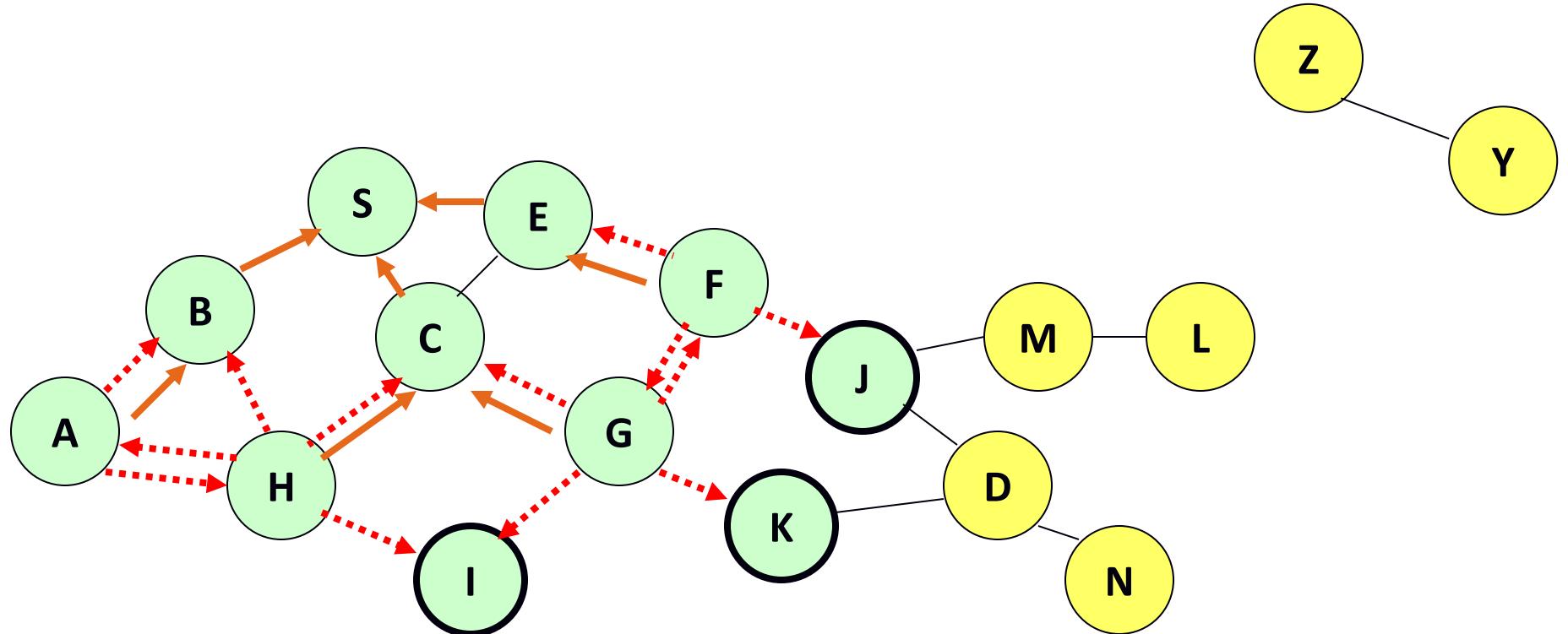


AODV - route request



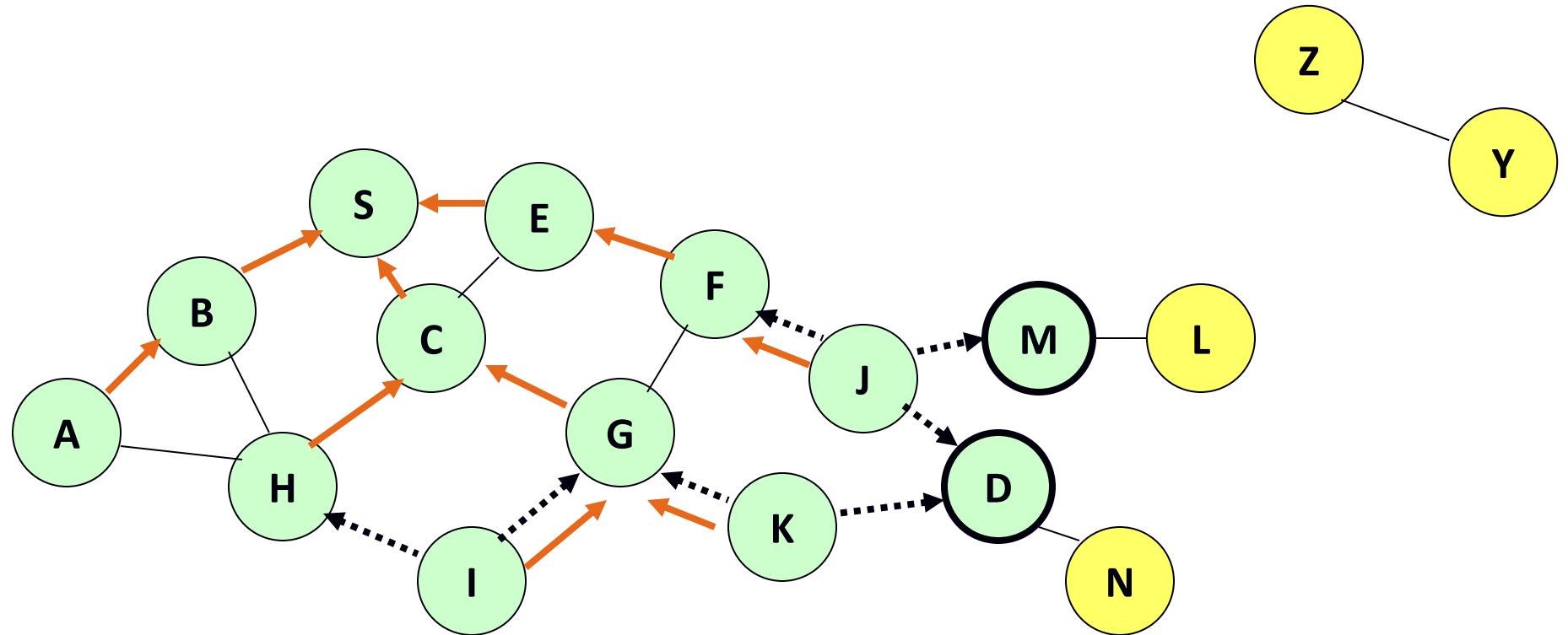
Oznaka pokazivača na prethodni čvor
od koga je primljen RREQ

AODV - route request

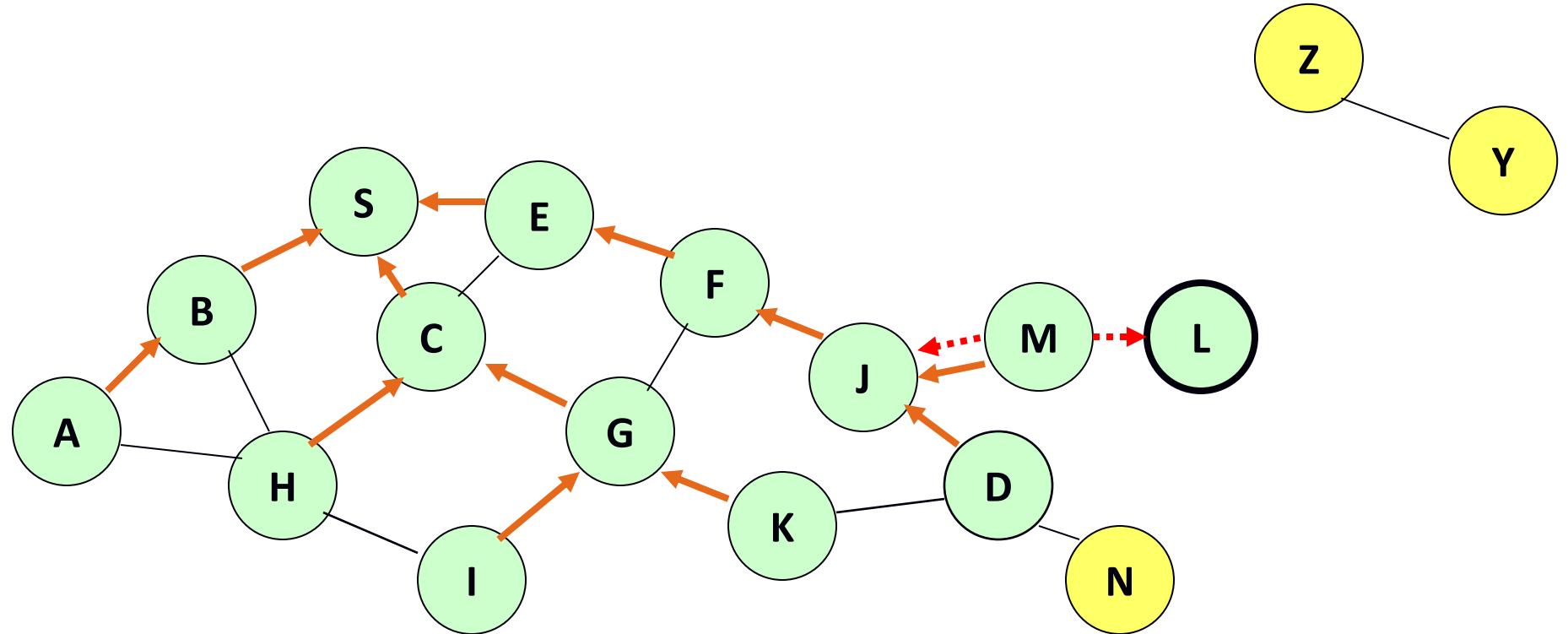


- Čvor H definira pokazivač na C (može birati između čvorova B i C)
- Čvor C prima RREQ od G i H, ali ga ne proslijedi ponovo, jer je C prethodno proslijedio isti RREQ (reagiraju samo I, J i K jer primaju RREQ prvi puta)

AODV - route request

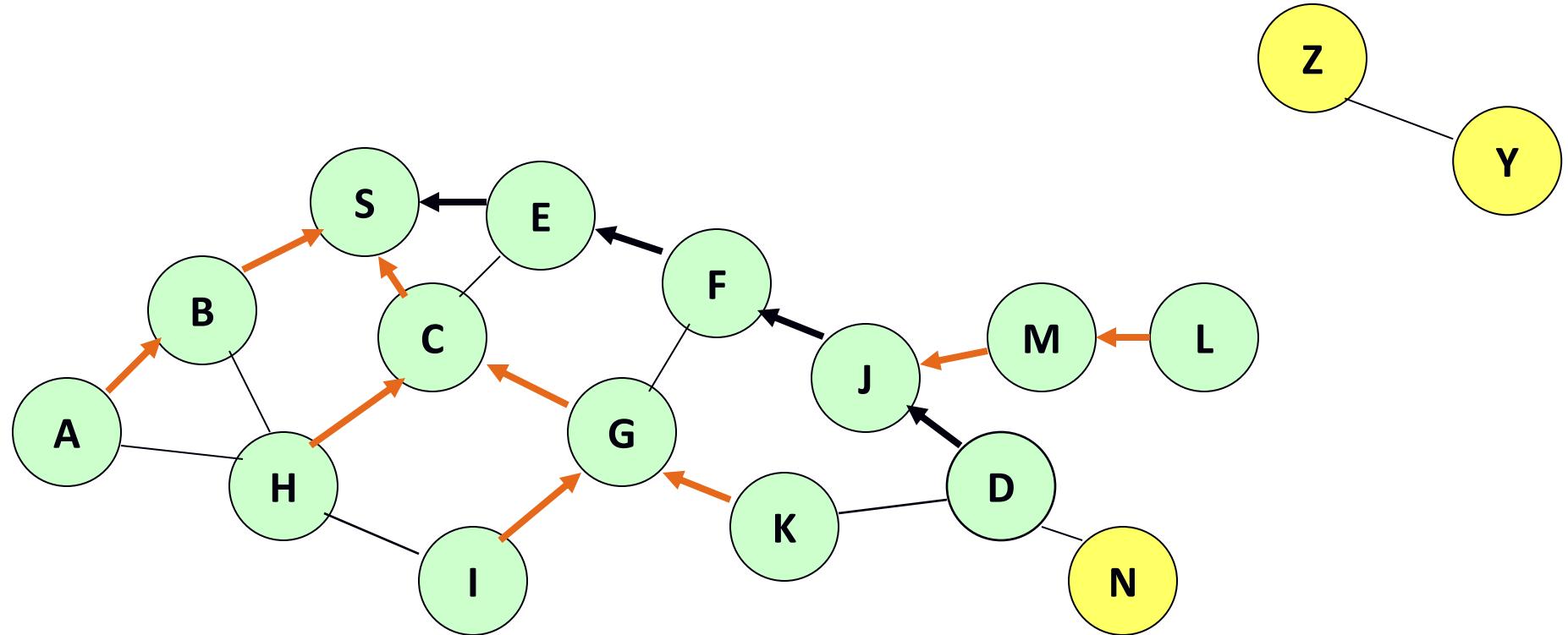


AODV - route request



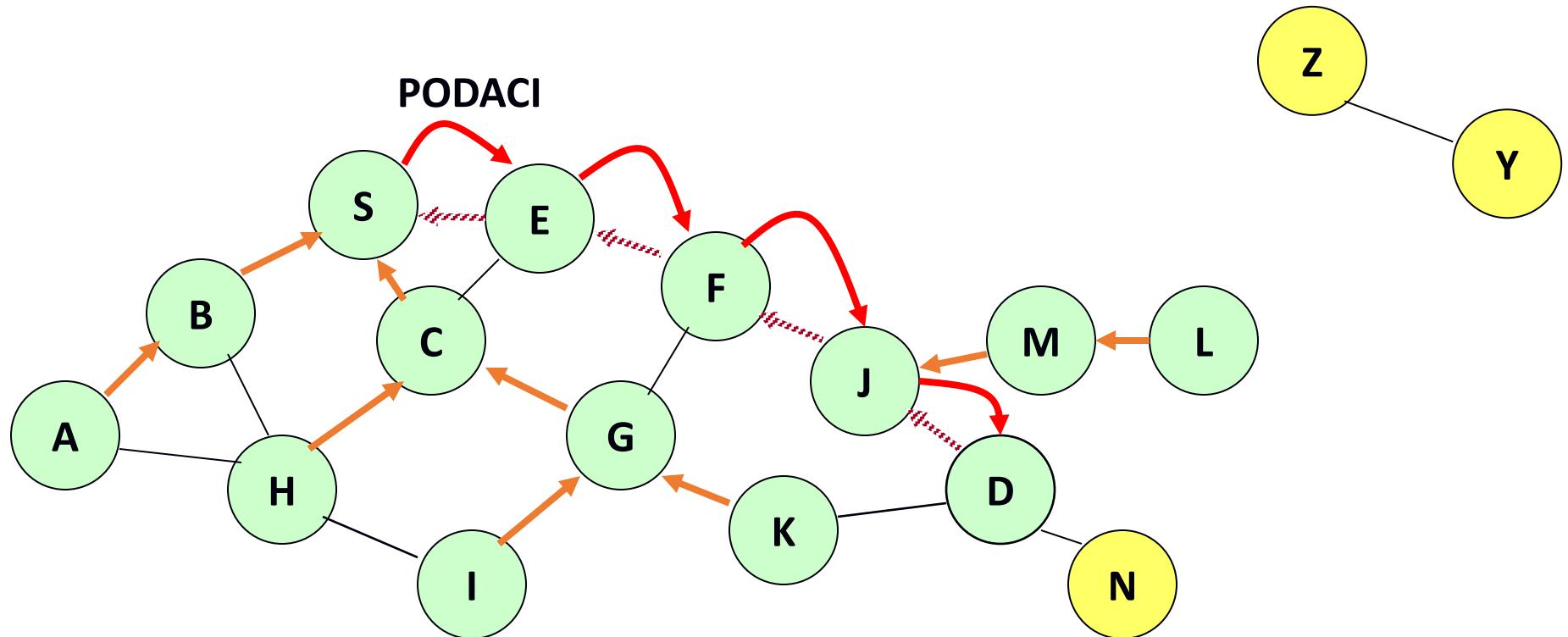
- Čvor D ne prosljeđuje RREQ dalje jer je D odredišni čvor

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
 - Jeden 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



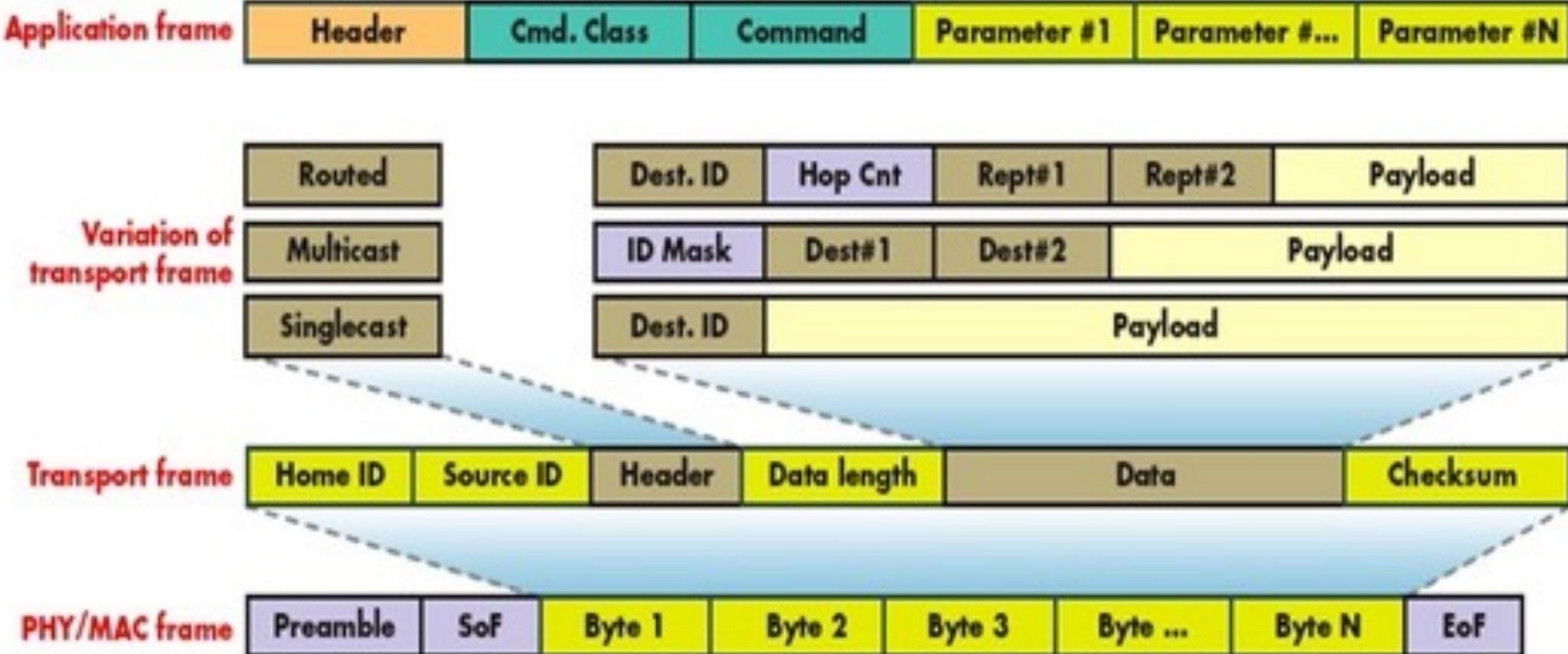
- Razvila ga privatna firma Zensys (2005.) Danska
 - kupila ih Sigma 2008., a prodani su Silicon Labsu 2018.
 - Jedini rade čipove
- Certifikacija kroz Z-Wave Alliance - 1700 proizvoda od 300 proizvođača
 - Specifikacija je [ovdje](#)
- Primjena u pametnom domu
- Frekvencija <GHz (868 MHz Europa, 908 US)
- Maksimalna udaljenost 30-100m (ovisi o zaprekama) – Z-Wave Plus 167m
- Brzina prijenosa: 9,6-100 Kb/s
- Koristi enkripciju AES 128
- Jeden 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 – prihvataju 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



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 $< 1\text{GHz}$
- 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) klase 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?
- Koja je razlika između ZigBeeja i Z-Wavea?
- Što je IEEE 802.11ah i koja su mu svojstva?



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)

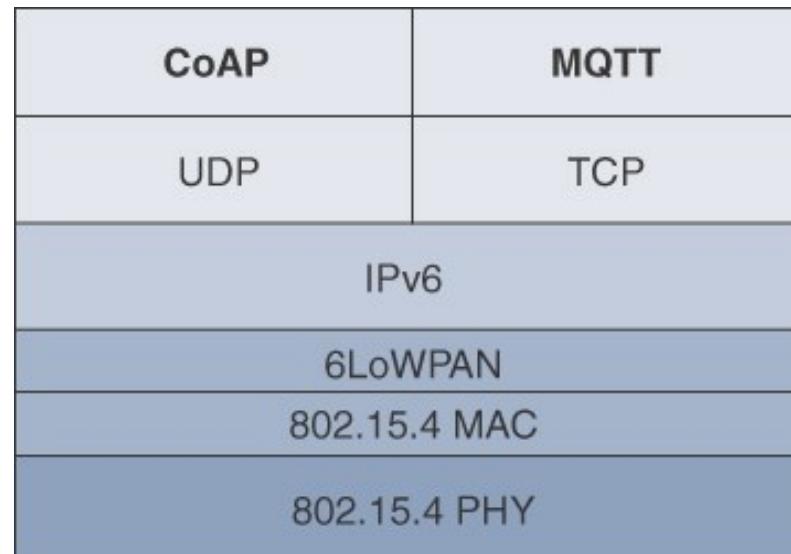
Internet stvari

4. Aplikacijski sloj: MQTT, CoAP

Ak. god. 2022./2023.

Sadržaj

- CoAP i MQTT
- Detaljni pregled dva aplikacijska protokola za uređaje i mreže ograničenih resursa



Constrained Application Protocol (CoAP)

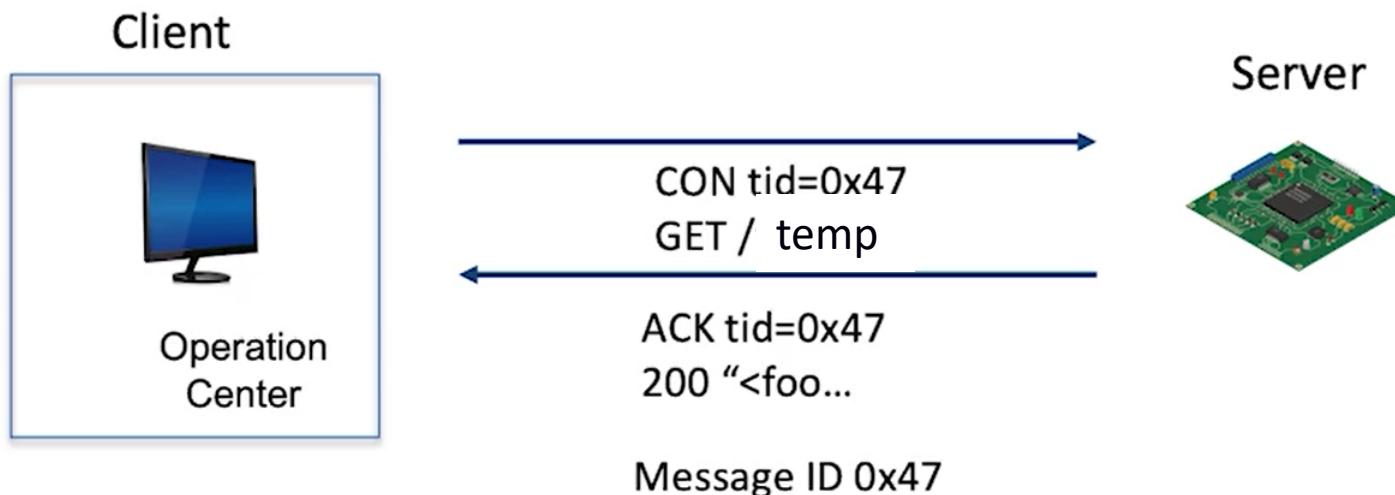
- CoAP *framework* definira jednostavne i fleksibilne načine za slanje i primanje podataka s IoT-uređaja te njihovo upravljanje
- IETF working group Constrained RESTful Environments (CoRE)
 - RFC 6690: Constrained RESTful Environments (CoRE) Link Format
 - RFC 7252: The Constrained Application Protocol (CoAP)
 - RFC 7641: Observing Resources in the Constrained Application Protocol (CoAP)
 - RFC 7959: Block-Wise Transfers in the Constrained Application Protocol (CoAP)
 - RFC 8075: Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP)
 - Ostali relevantni dokumenti: <http://datatracker.ietf.org/wg/core/>

CoAP

- Protokol je definiran u [RFC 7252](#)
- Resursi se identificiraju pomoću URI-ja, IoT-uređaj postaje poslužitelj koji nudi resurse
- Temelji se na REST-u (metode **GET, POST, PUT i DELETE**)
- Klijenti pristupaju resursima pomoću asinkronog mehanizma zahtjev-odgovor
- Koristi UDP kao transportni protokol i poseban “message layer” za retransmisiju izgubljenih paketa
- Koristi tehnikе za kompresiju podataka
- Sigurna komunikacija omogućena protokolom DTLS (Datagram Transport Layer Security)

`coap://mymeter.com:5683/ temp`

1. način rada: zahtjev-odgovor



2. način rada: promatraj



CoAP URI

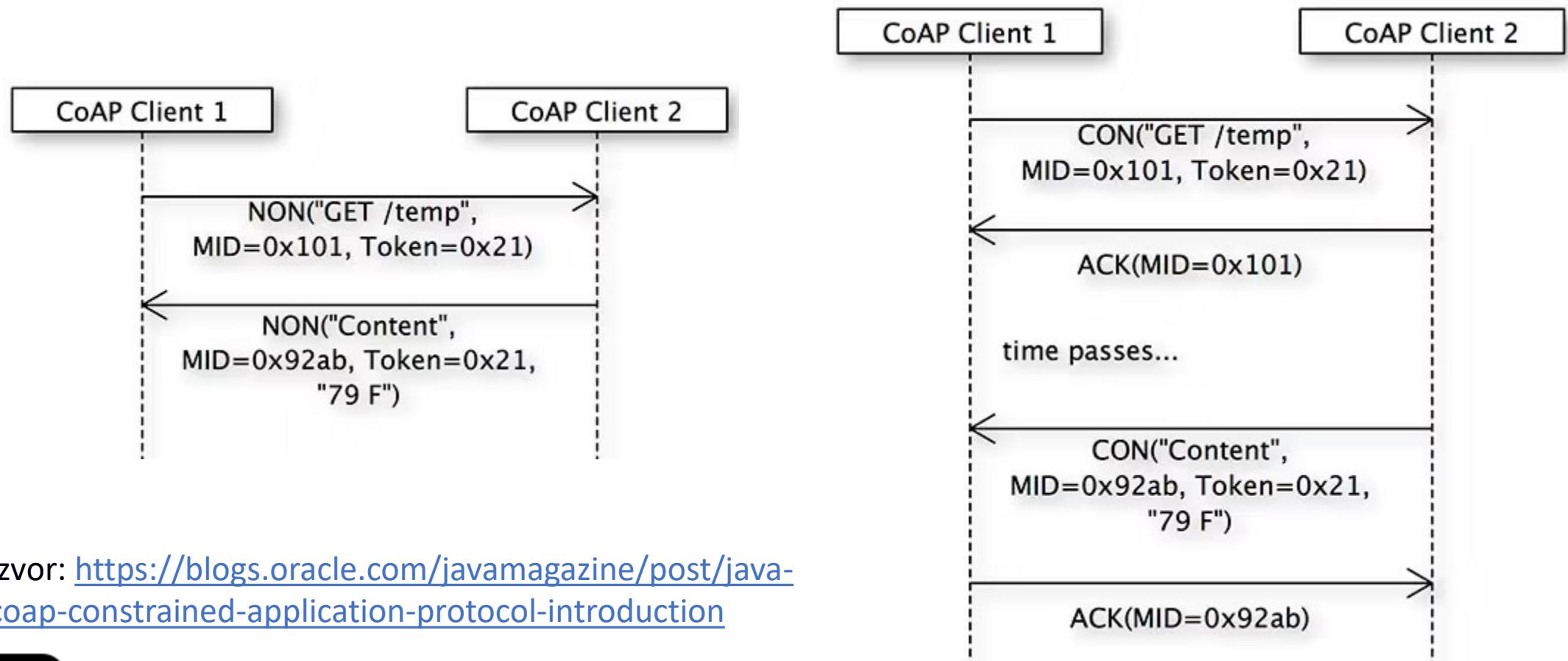
- URI se sastoji od sljedećih segmenta
 - coap[s]://<host>[:<port>]/<path>[?<query>]
URI schema + authority + path + query

- CoAP URI
 - coap://example.smarthome.com:5683/sensors
- CoAPs URI
 - coaps://example.smarthome.com:5684/activate_alarm

Vrste CoAP poruka

Type	Description
CON	Confirmable Message Each confirmable message is acknowledged either by a message type of "Ack" or "Reset".
NON	Non-Confirmable Message For messages that do not require an acknowledgement. This is particularly true for messages that are repeated regularly for application requirements, such as repeated readings from a sensor where eventual success is sufficient.
Ack	Acknowledgement Message An Ack acknowledges that a specific CON message arrived. It does not indicate success or failure of any encapsulated request.
Reset	Reset Message A Reset message indicates that a specific message (CON or NON) was received, but some context is missing to properly process it. This condition is usually caused when the receiving node has rebooted and has forgotten some state that would be required to interpret the message. Provoking a Reset message (e.g., by sending an empty Confirmable message) is also useful as an inexpensive check of the liveness of an endpoint ("CoAP ping").

Osnovna interakcija: zahtjevi NON i CON



Izvor: <https://blogs.oracle.com/javamagazine/post/java-coap-constrained-application-protocol-introduction>

Metode CoAP-a

- **GET**

- The GET method retrieves a representation for the information that currently corresponds to the resource identified by the request URI.
- The GET method is safe and idempotent.

- **POST**

- The POST method requests that the representation enclosed in the request be processed.
- POST is neither safe nor idempotent.

- **PUT**

- The PUT method requests that the resource identified by the request URI be updated or created with the enclosed representation.
- PUT is not safe, but is idempotent.

- **DELETE**

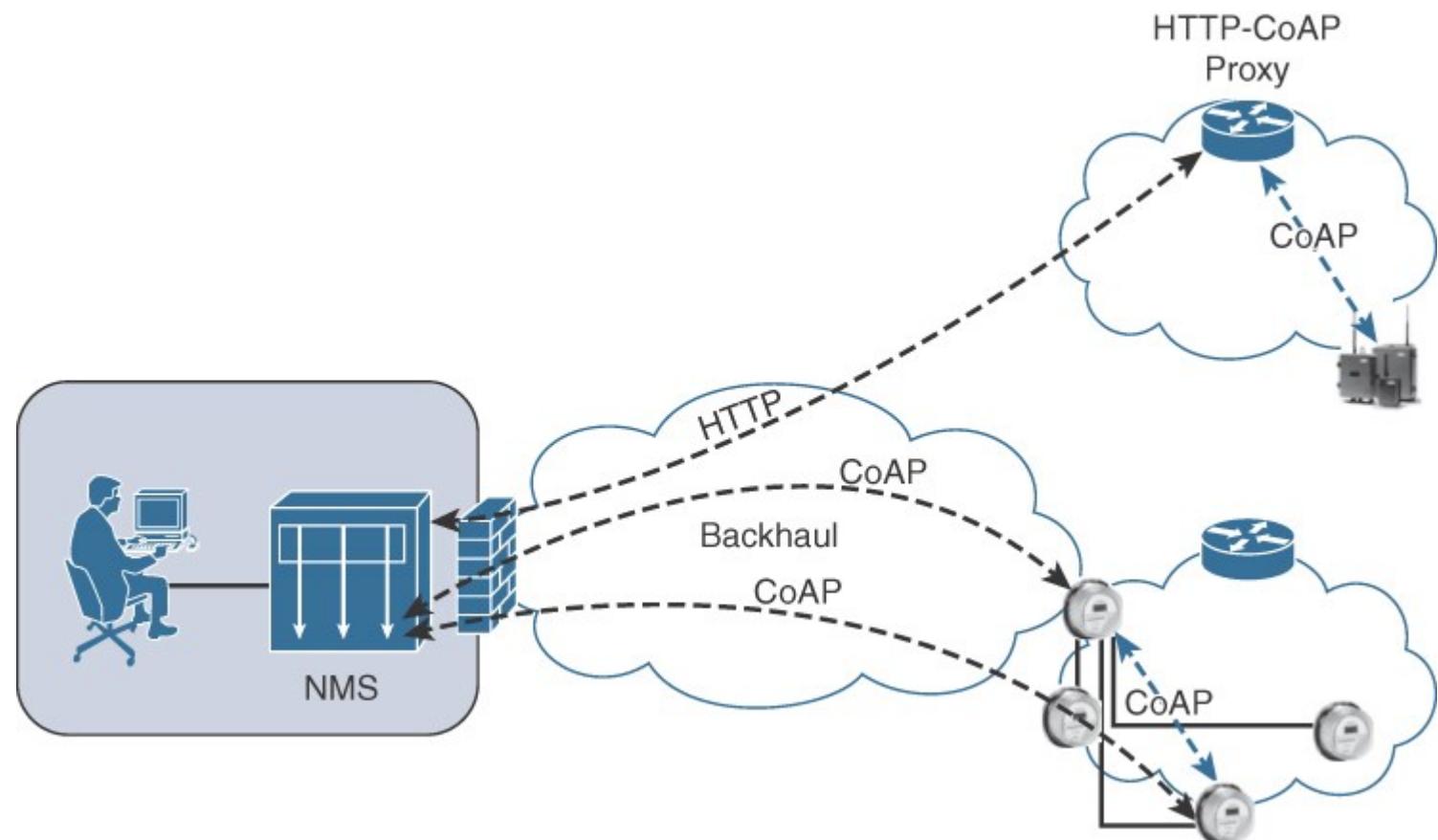
- The DELETE method requests that the resource identified by the request URI be deleted.
- DELETE is not safe, but is idempotent.

Prijenos poruka

- Poruka nosi sljedeće: zahtjev, odgovor ili je prazna
- CoAP *endpoint* (IP address, UDP port) : izvor ili odredište poruke
- Poruke se razmjenjuju asinkrono
- Mehanizam za pouzdanu isporuku poruka je relativno jednostavan
 - *stop-and-wait-retransmission*, vrijeme čekanja na poruke se eksponencijalno povećava (vrijedi samo za poruke tipa *Confirmable*)
 - koristi se i brojač MAX_RETRANSMIT
 - detekcija duplikata (za poruke tipa *Confirmable* i *Non Confirmable*)

CoAP: protokolni složaj i „suživot” s HTTP-om

- Komunikacija među uređajima unutar jedne podmreže ili putem javnog Interneta
- Definiran je Proxy mehanizam u RFC 8075 koji mapira HTTP poruke u CoAP poruke



Prednosti i nedostaci CoAP-a

Prednosti

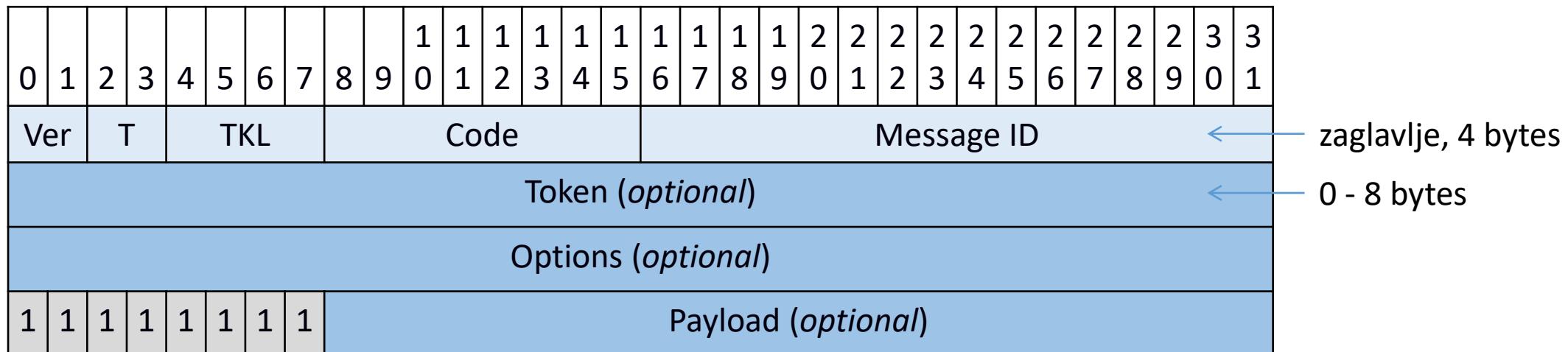
- Prilagođen uređajima i mrežama ograničenih resursa (koristi UDP)
- Vrlo niska potrošnja energije, može se koristiti u okolinama s ograničenim napajanjem (baterija)
- Temelji se na REST-u
- Omogućuje potvrdu poruke (QoS)
- DTLS za šifriranje poruka

Nedostaci

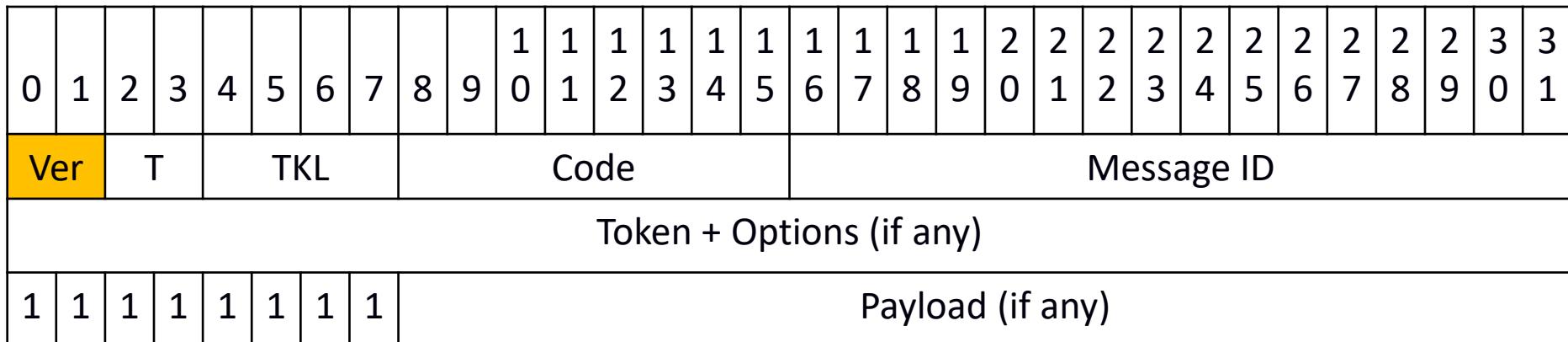
- Komunikacija je uvijek 1 na 1 (jedan izvor i jedno odredište)

Format CoAP poruke

- RFC 7252 definira sadržaj svakog CoAP okvira
 - **coap** (non-secured CoAP) koristi vrata 5683
 - **coaps** (DTLS-secured CoAP) koristi vrata 5684
 - podrška i za ostale transportne protokole: SMS, TCP, SCTP,...



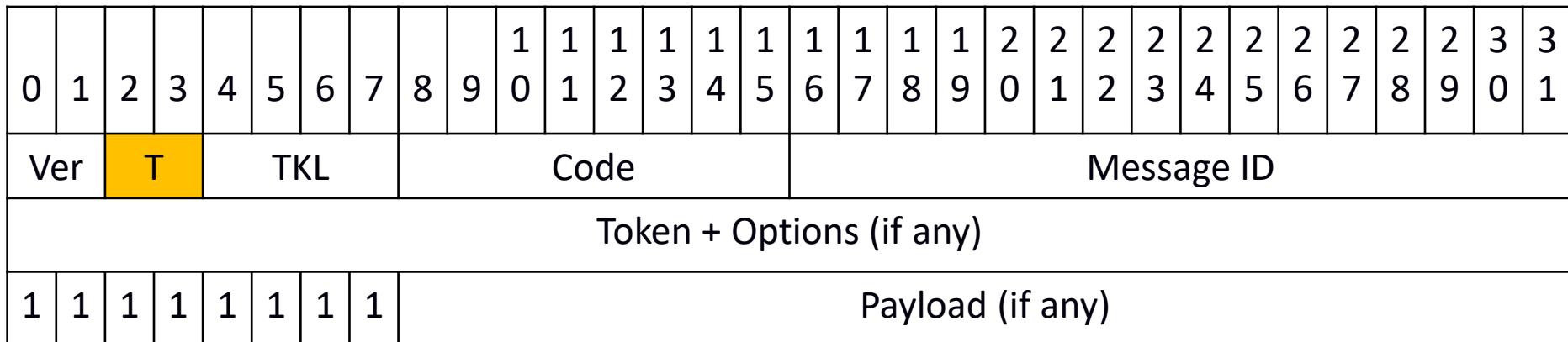
Objašnjenje zaglavljaja CoAP poruke



- **Version (Ver)**

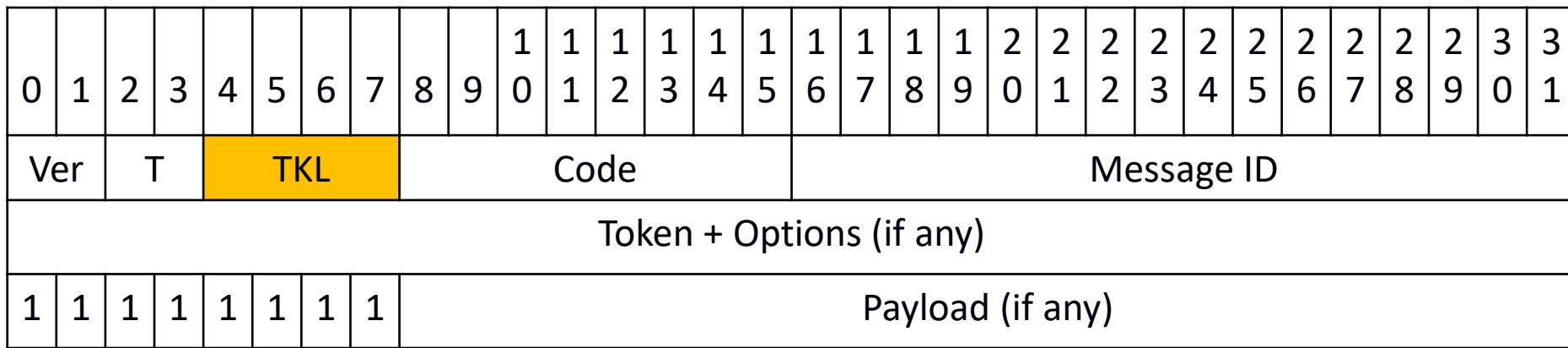
- 2-bitni prirodni broj
- predstavlja verziju CoAP protokola
- prema trenutnoj specifikaciji mora biti postavljen na 01
- nespecificirane verzije MORAJU biti ignorirane

Objašnjenje zaglavljaja CoAP poruke



- **Type (T)**
 - 2-bitni prirodni broj
 - predstavlja jedan od tipova poruka:
 - Confirmable (0)
 - Non-confirmable (1)
 - Acknowledgement (2)
 - Reset(3)

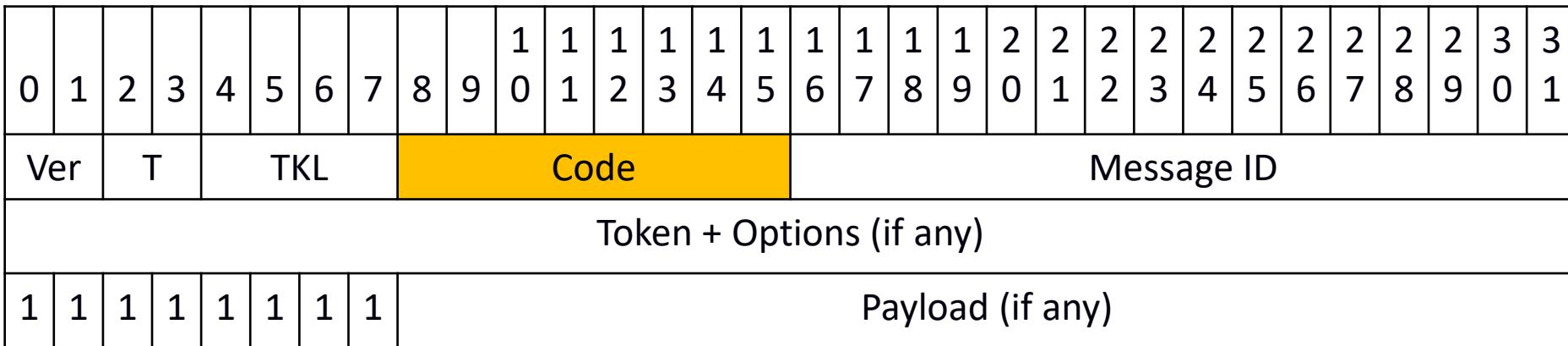
Objašnjenje zaglavljaja CoAP poruke



- **Token Length (TKL)**

- 4-bitni prirodni broj
- predstavlja duljinu polja Token
- Token se koristi za povezivanje zahtjeva i njegovog odgovora te je neovisan o *Message ID*
- *A token is intended for use as a client-local identifier for differentiating between concurrent requests; it could have been called a "request ID". The client SHOULD generate tokens in such a way that tokens currently in use for a given source/destination endpoint pair are unique.*

Objašnjenje zaglavlja CoAP poruke



- 8-bitni prirodni broj
 - podjela u dvije cjeline: *3-bit class* (najznačajniji bitovi) i *5-bit detail* (manje značajni bitovi)
 - notacija: „*c.dd*” gdje je *c* broj od 0 – 7, a *dd* broj od 00 – 31
 - klase mogu biti:
 - Request (0)
 - Success response (2)
 - Client error response (4)
 - Server error response (5)
 - Posebni slučaj poruke je 0.00 koji predstavlja praznu poruku (*Empty message*)
 - u slučaju upita (*Request*) polje *Code* predstavlja *Request code*, a u slučaju odgovora (*Response*) predstavlja *Response code*

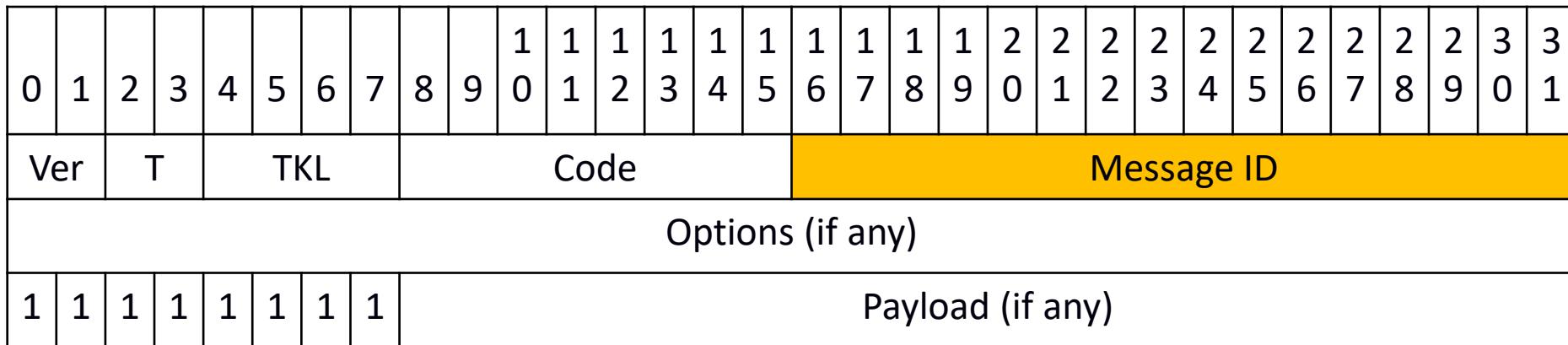
CoAP kodovi zahtjeva i odgovora

Općenita podjela	
Kod	Opis
0.00	Kod prazne poruke
0.01 – 0.31	Kodovi zahtjeva
1.00 – 1.31	Rezervirani kodovi
2.00 – 5.31	Kodovi odgovora
6.00 – 7.31	Rezervirani kodovi

Kodovi zahtjeva	
Kod	Opis
0.01	GET
0.02	POST
0.03	PUT
0.04	DELETE
0.05 – 1.31	Nedodijeljeni kodovi

Kodovi odgovora					
Kod	Opis	4.01	Unauthorized	4.14	Nedodijeljen kod
2.00	Nedodijeljen kod	4.02	Bad option	4.15	Unsupported Content-Format
2.01	Created	4.03	Forbidden	4.16 – 4.31	Nedodijeljeni kodovi
2.02	Deleted	4.04	Not found	5.00	Internal Poslužitelj Error
2.03	Valid	4.05	Method not allowed	5.01	Not Implemented
2.04	Changed	4.06	Not acceptable	5.02	Bad Gateway
2.05	Content	4.07 – 4.11	Nedodijeljeni kodovi	5.03	Service Unavailable
2.06 – 2.31	Nedodijeljeni kodovi	4.12	Precision failed	5.04	Gateway Timeout
3.00 – 3.31	Rezervirani kodovi	4.13	Request entity too large	5.05	Proxying Not Supported
4.00	Bad request			5.06 – 5.31	Nedodijeljeni kodovi

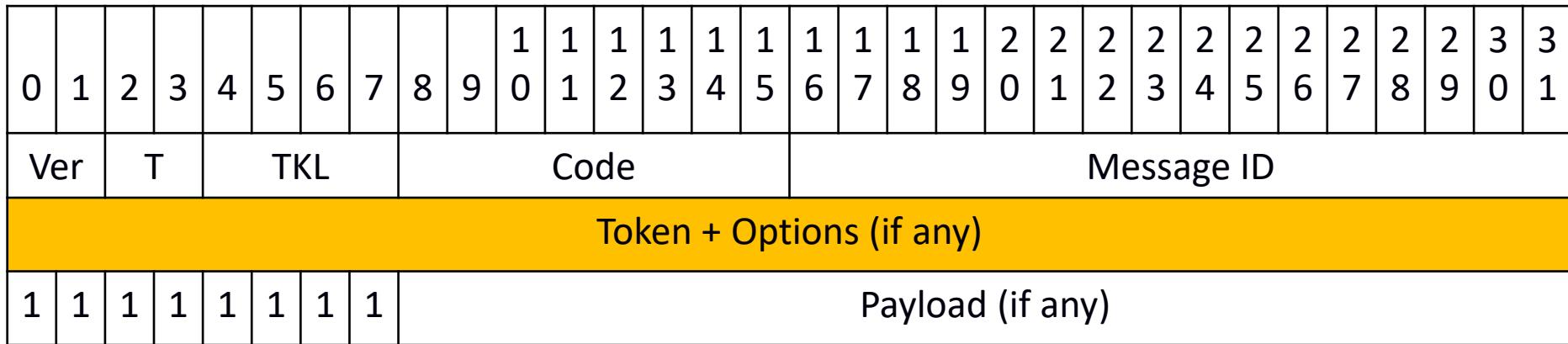
Objašnjenje zaglavljaja CoAP poruke



- ***Message ID***

- 16-bitni prirodni broj
- za detekciju višestrukih poruka i povezivanje poruka tipa *Acknowledgement/Reset* s porukama tipa *Confirmable/Non-confirmable*

Objašnjenje zaglavlja CoAP poruke

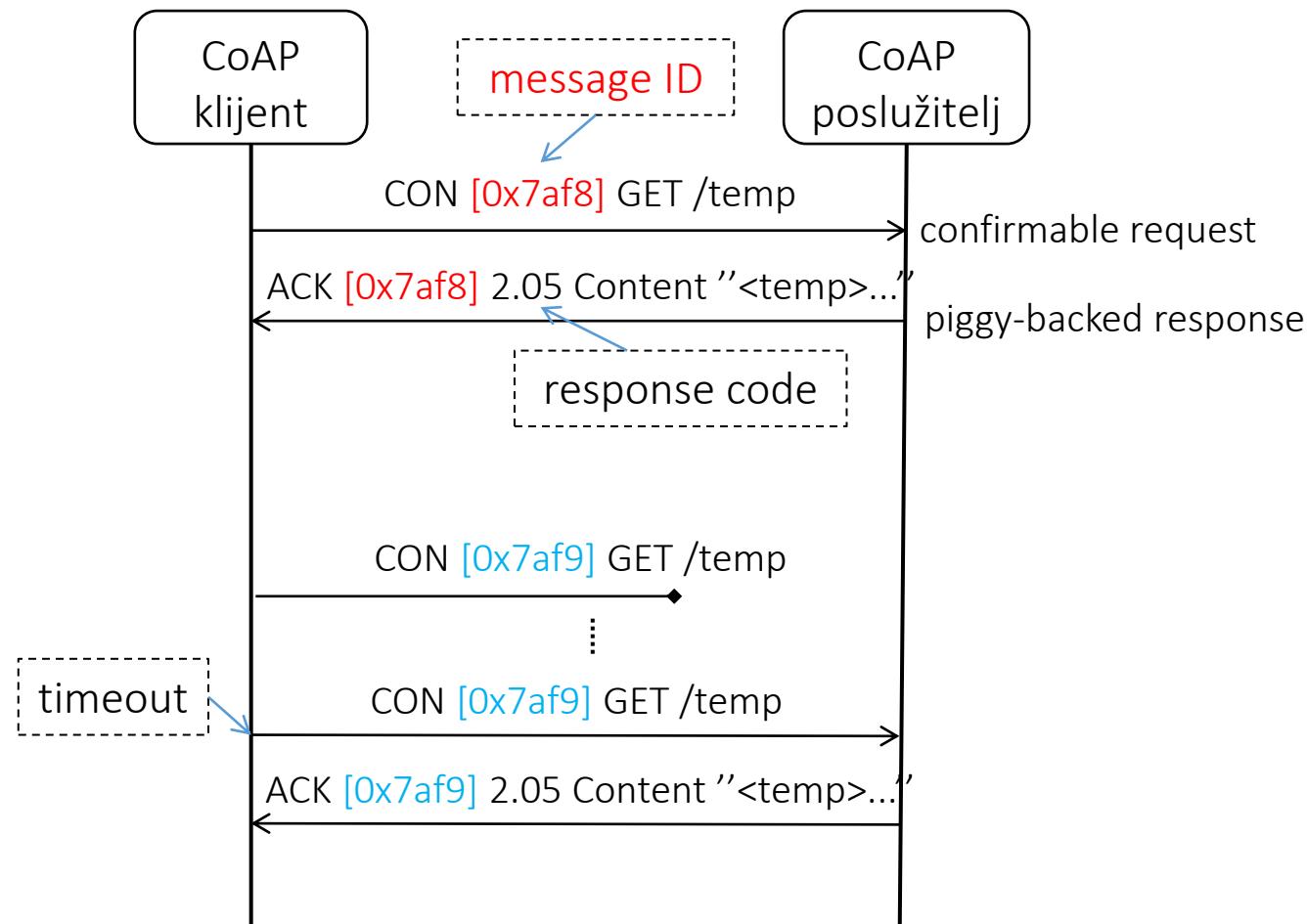


- Token se koristi za povezivanje zahtjeva i njegovog odgovora te je neovisan o *Message ID*
- svaka opcija mora biti u skladu sa specifikacijom, a sastoji se od:
 - Option number (delta) – 4-bitni prirodni broj
 - Option length – 4-bitni prirodni broj
 - Option value – sadrži jednu od sljedećih opcija:
 - Empty – niz bitova duljine 0
 - Opaque – nedefinirana struktura niza okteta
 - Uint – konačan niz okteta prikazan u polju *Option length*
 - String – niz znakova kodiran koristeći UTF8 (RFC3629)

*CoAP defines a single set of options that are used in both requests and responses: **Content-Format**, **Etag**, **Location-Path**, **Location-Query**, **Max-Age**, **Proxy-Uri**, **Proxy-Scheme**, **Uri-Host**, **Uri-Path**, **Uri-Port**, **Uri-Query**, **Accept**, **If-Match**, **If-None-Match**, **Size***

Npr. CoAP Content-Formats: text, utf-8, json, xml...

CoAP – confirmable request



Interakcija: zahtjev-odgovor

Request:

Header: GET (T=CON, Code=1, MID=0x7af8)

Uri-Path: "temp"

8-bitni zapis odgovora 2.05

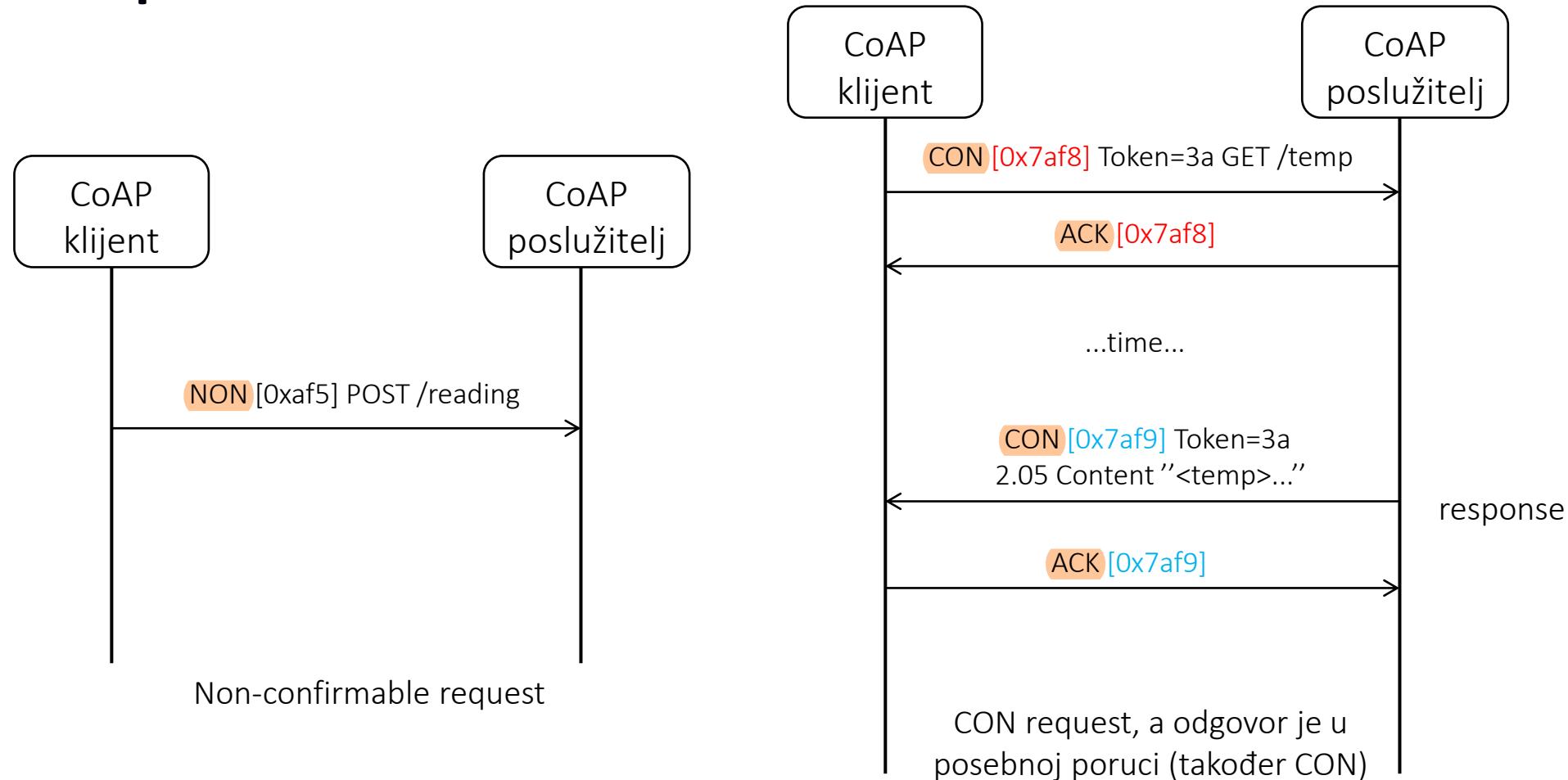
Response:

Header: 2.05 Content (T=ACK, Code=69, MID=0x7af8)

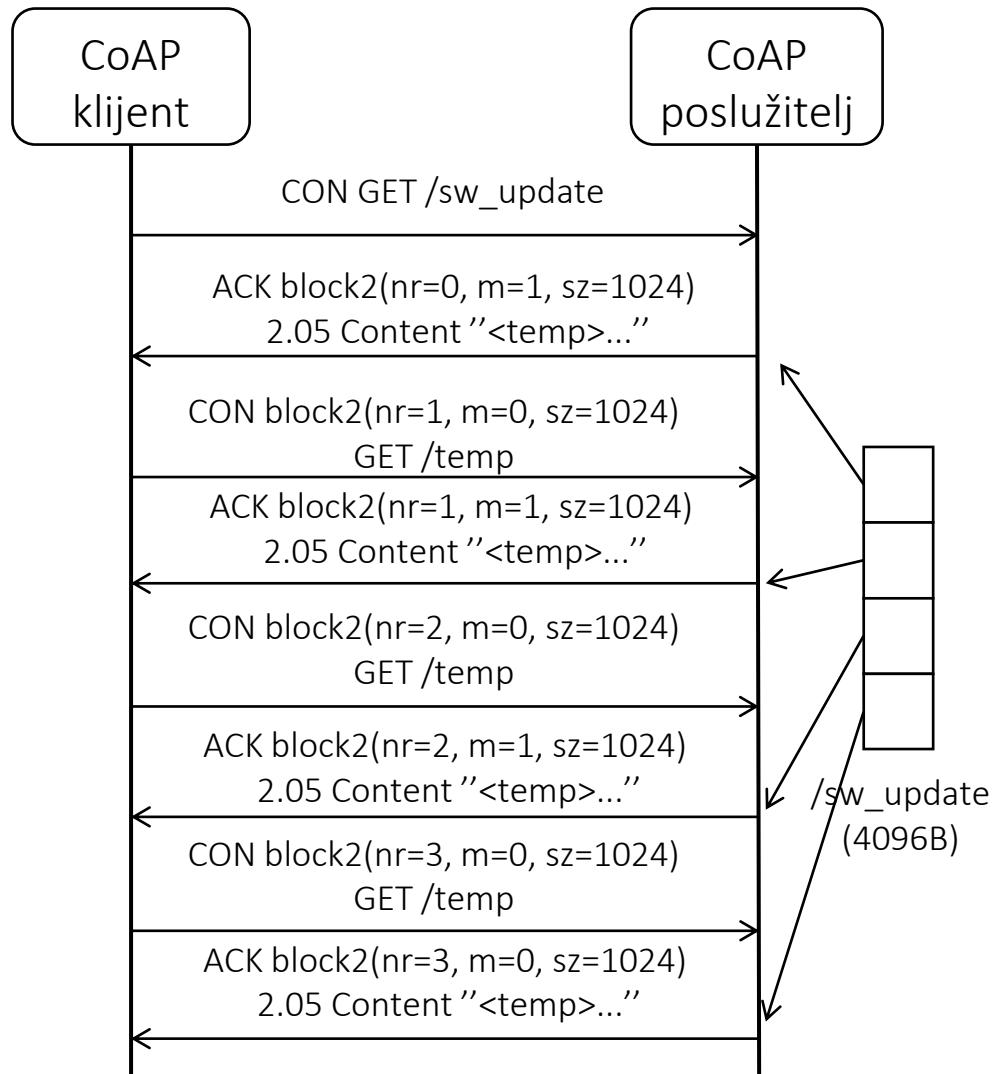
Payload: "<temp>22.3 C</temp>"

message ID omogućuje
detekciju duplih poruka

CoAP – non-confirmable request i separate response



CoAP – block transfer

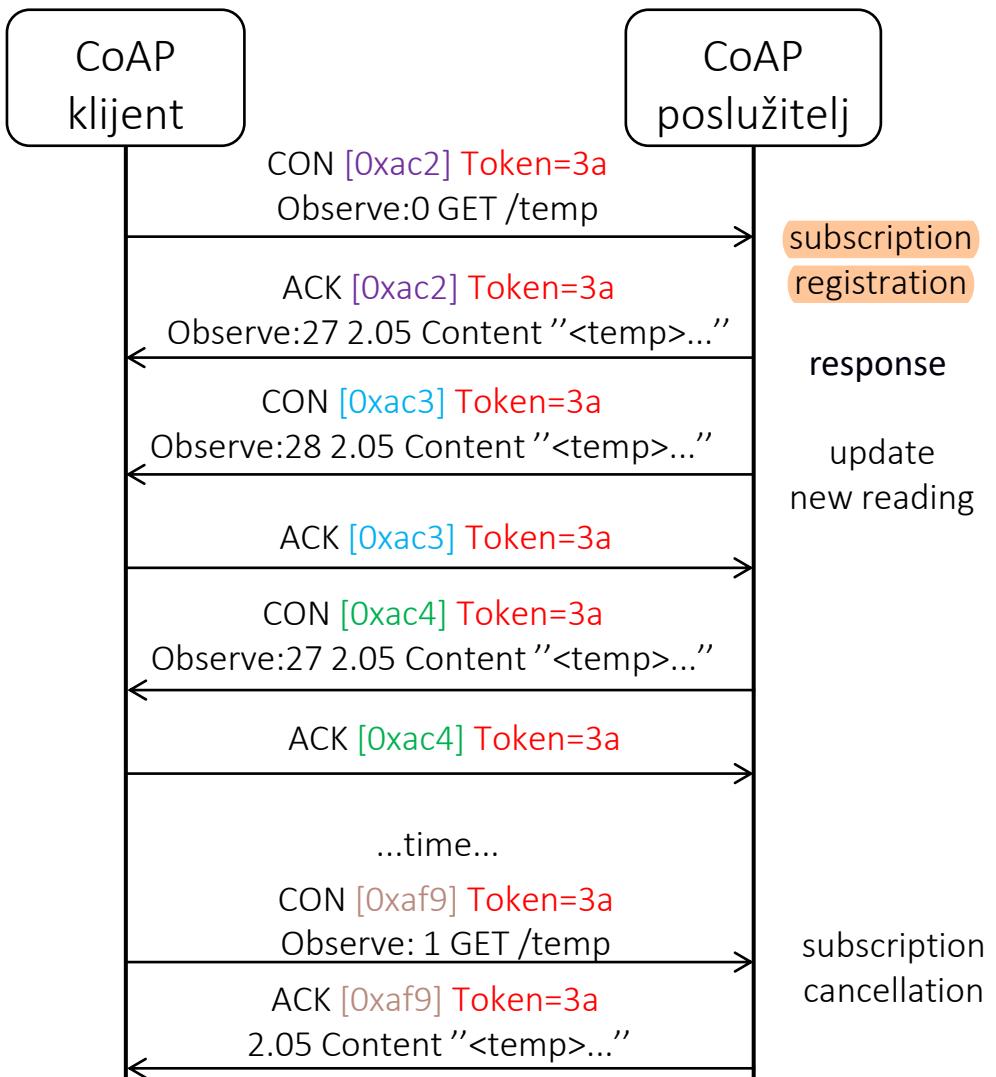


If you're required to send content that exceeds the amount of data possible to embed in a datagram, CoAP allows you to divide your content into **blocks**.

Whenever you send data using CoAP, you can also provide a **block size**. If the content exceeds this block size, the CoAP layer divides it into blocks and transmits them individually, while the receiving end assembles the blocks and delivers the complete payload to its application at the other end. Block-wise transfers using CoAP is defined in RFC 7959:

<https://tools.ietf.org/html/rfc7959>.

CoAP - observation



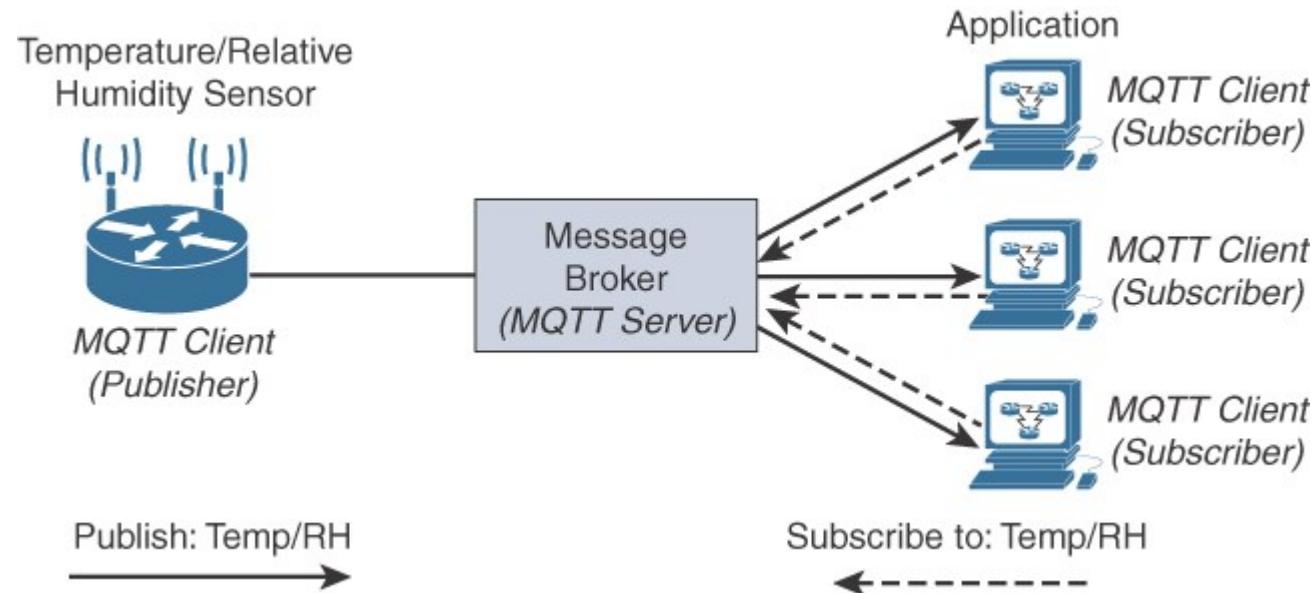
- Klijent registrira preplatu
- U odgovoru (ACK) se prenosi očitanje, a sljedeći odgovori se šalju bez eksplicitnog zahtjeva dok ne stigne poruka za otkazivanje preplate
- Smanjuje se generirani promet, očitanja se dostavljaju u trenutku nastanka
- Resursi koji podržavaju ovaj pattern se zovu *observable resources*, definirano u RFC 7641:
<https://tools.ietf.org/html/rfc7641>

Message Queuing Telemetry Transport (MQTT)

- Jednostavan protokol za prijenos poruka na načelu **objavi-preplati** prilagođen uređajima i mrežama s ograničenim resursima
- Dodaje mali transportni overhead (header je veličine 2 byte), „*lightweight protocol*”
- Koristi **TCP/IP** na mrežnom sloju (najčešće, moguće izvedbe putem UDP-a)
- <http://mqtt.org>
- MQTT je standard koji definira OASIS (Organization for the Advancement of Structured Information Standards)
 - posljednja verzija standarda [MQTT v5.0](#), 7.3.2019.
 - prethodna verzija [MQTT v3.1.1](#), 10.12.2015.

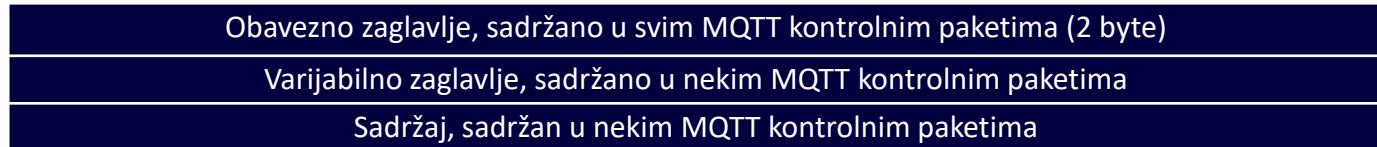
Osnovni komunikacijski mehanizam

- **MQTT Broker**: posrednik između objavljivača i pretplatnika (poslužitelj)
- **MQTT Client**
 - **Publisher**: objavljuje poruke na *Topic*
 - **Subscriber**: pretplaćuje se na *Topic*, prima objavljene poruke putem Brokera nakon što ih posrednik primi od objavlivača
 - 1 poruka se potencijalno isporučuje do n pretplatnika



Kontrolni paketi

- Sastoje se od zaglavlja fiksne duljine (2 byte) nakon čega može slijediti:
 - *varijabilno zaglavje*
 - *sadržaj* (do 256 MB)
- MQTT prenosi **kontrolne** pakete putem **TCP-a** (port 1883)
- TCP osigurava **ispravan prijenos** paketa bez gubitaka
- MQTT se može koristiti u kombinaciji s TLS-om (port 8883)
- Za prijenos se također može koristiti WebSocket (definirano u RFC 6455)
- *Durable Sessions*: omogućuju perzistentnost poruka (*Store and Forward*)



MQTT-sjednica

- Ostvaruje se između svakog klijenta i brokera
- Sastoji se od 4 faze:
 - *session establishment*,
 - *authentication*,
 - *data exchange*,
 - *session termination*.
- Svaki klijent se identificira jedinstvenim identifikatorom koji služi i za identifikaciju otvorene sjednice
- Prilikom isporuke poruke do više klijenata, broker će svaku isporuku obaviti neovisno o ostalim sjednicama

Vrste poruka

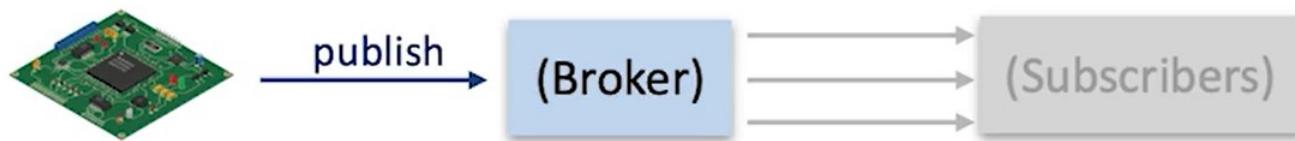
- Preplate na temu generiraju kontrolne pakete **SUBSCRIBE/SUBACK**
- Brisanje preplate na temu se ostvaruje pomoću **UNSUBSCRIBE/UNSUBACK**
- Slanje podataka i potvrda primanja **PUBLISH/PUBACK**
- Za zatvaranje konekcije se koristi **DISCONNECT**
 - jedina poruka iza koje ne slijedi ACK
 - slanjem client ID-ja se ostvaruje reconnect
- Za održavanje sjednice (zbog konekcije TCP-a) se koriste **PINGREQ/PINGRESP**
 - provjera da je klijent još uvijek dostupan
- **PUBREC** i **PUBREL** (objašnjene na sl. 29)

Razine QoS-a (1/2)

- **Razina 0** (najniža, *best effort*) uključuje isporuku poruke **najviše jedan put**, pri čemu je moguće da poruka **uopće ne stigne** do odredišta.
 - *At most once*, koristi se samo PUBLISH
- **Razina 1** uključuje isporuku **barem jedan put**, pri čemu je moguće primanje više od jedne poruke. Moguće su **duple poruke**.
 - *At least once*, koriste se PUBLISH i PUBACK, a u varijabilnom zaglavlju piše *packetID*.
 - Ako ne stigne PUBACK, PUBLISH se ponavlja.
- **Razina 2** uključuje isporuku poruke **točno jedan put**.
 - *Exactly once*, ova razina ima značajan *overhead* i zahtijeva ACK u dva koraka

Razine QoS-a (2/2)

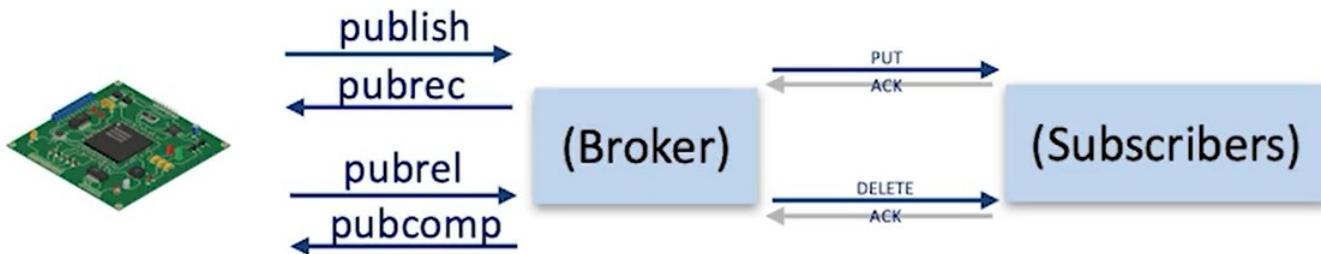
At most once:



At least once:



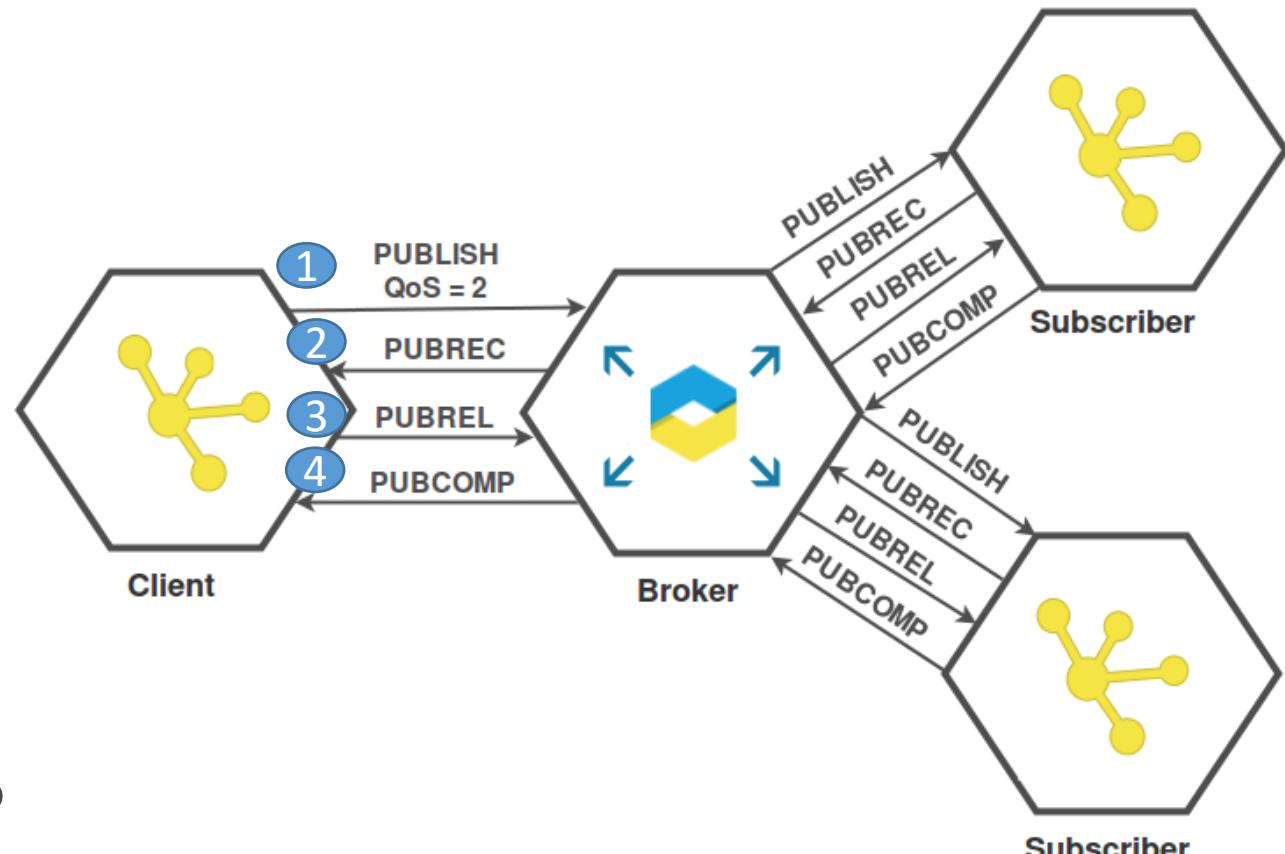
Exactly once:



Poruke za QoS=2

1. Klijent šalje PUBLISH s QoS=2.
2. Broker pohranjuje poruku i odgovara s PUBREC klijentu.
3. Klijent šalje brokeru PUBREL.
4. Broker pohranjuje poruku i odgovara s PUBCOMP.
5. Nakon primitka poruke, broker ponavlja isporuku u dva koraka PUBLISH/PUBREC i PUBREL/PUBCOMP do svakog pretplatnika.

<https://www.iotbroker.cloud/blog/MQTT/Publish%20message%20flow%20and%20levels%20of%20QoS%20in%20MQTT>



Jezik za pretplate

- Temelji se na hijerarhiji tema (*topic*), teme u hijerarhiji se odvajaju znakom /
 - Npr. FER/C08-18/sensors/temperature, FER/C08-18/sensors/humidity
 - Klijent-objavljavač ne mora prije slanja prve poruke na temu konfigurirati novu temu na brokeru, samo šalje poruku i definira temu
- Primjeri pretplate
 - FER/C08-18/sensors/temperature (samo na jednu temu)
 - FER/# (sve teme) koje počinju s FER, # označava sve preostale stupnjeve hijerarhije)
 - FER/C08-18/# (sve teme) registrirane za FER/C08-18, npr. svi senzori i aktuatori)
 - FER/+/sensors/+ (pretplata na sve senzore na FER-u, + označava samo jedan stupanj u hijerarhiji)

Dodatni koncepti

- *Clean Session*
 - ako je *clean session flag* = 1 kada se ostvaruje sjednica, sve definirane pretplate tijekom sjednice će biti uklonjene s brokera nakon njenog zatvaranja
 - ako je *clean session flag* = 0 pretplate ostaju definirane i nakon zatvaranja sjednice
- *Durable Connections*
 - Kada je *clean session flag* = 0, sve poruke isporučene brokeru za vrijeme kada je klijent odspojen koje imaju QoS>0 će biti pohranjene na brokeru i isporučene nakon što se klijent ponovno spoji
- *Will flag*
 - definira pravila u slučaju neočekivanog prekida konekcije, postavlja klijent kada kreira sjednicu
 - MQTT v5.0 definira *Session expiry* i *Message expiry*

MQTT: format zaglavlja

Zaglavje,
2 byte

bit	7	6	5	4	3	2	1	0
byte 1					Message Type	DUP flag	QoS level	RETAIN
byte 2						Remaining Length		

- **CONNECT** (klijent -> poslužitelj) – klijent poslužitelju šalje zahtjev za otvaranje konekcije;
- **CONNACK** (poslužitelj -> klijent) – poslužitelj klijentu šalje potvrdu o stvaranju konekcije;
- **PUBLISH** (klijent -> poslužitelj, poslužitelj -> klijent) – slanje poruke;
- **PUBACK** (klijent -> poslužitelj, poslužitelj -> klijent) – potvrda o slanju poruke;
- **PUBREC*** (klijent -> poslužitelj, poslužitelj -> klijent) – PUBLISH RECeived, potvrda o primanju poruke;
- **PUBREL*** (klijent -> poslužitelj, poslužitelj -> klijent) – PUBLISH RELease, potvrda za otpuštanje poruke;
- **PUBCOMP*** (klijent -> poslužitelj, poslužitelj -> klijent) – PUBLISH COMPlete, potvrda o uspješnom prijenosu poruke, posljednja potvrda ra QoS=2;

*poruke se koriste kod sigurnog isporučivanja (engl. *assured delivery*), vezano uz QoS level

MQTT: format zaglavlja

Zaglavlje,
2 byte

bit	7	6	5	4	3	2	1	0
byte 1					Message Type	DUP flag	QoS level	RETAIN
byte 2						Remaining Length		

- **SUBSCRIBE** (klijent -> poslužitelj) – klijent poslužitelju šalje zahtjev za pretplatom;
- **SUBACK** (poslužitelj -> klijent) – poslužitelj klijentu šalje potvrdu o pretplati;
- **UNSUBSCRIBE** (klijent -> poslužitelj) – klijent poslužitelju šalje zahtjev za brisanjem pretplate;
- **UNSUBACK** (poslužitelj -> klijent) – poslužitelj klijentu šalje potvrdu o brisanju pretplate;
- **PINGREQ** (klijent -> poslužitelj) – klijent šalje poslužitelju PING zahtjev (za održavanje TCP konekcije);
- **PINGRESP** (poslužitelj -> klijent) – poslužitelj odgovara klijentu na PING zahtjev;
- **DISCONNECT** (klijent -> poslužitelj) – klijent zatvara konekciju prema poslužitelju.

MQTT: kodovi za Message Type

Mnemonic	Enumeration	Description
Reserved	0	Reserved
CONNECT	1	Client request to connect to Server
CONNACK	2	Connect Acknowledgment
PUBLISH	3	Publish message
PUBREC	5	Publish Received (assured delivery part 1)
PUBREL	6	Publish Release (assured delivery part 2)
PUBCOMP	7	Publish Complete (assured delivery part 3)
SUBSCRIBE	8	Client Subscribe request
SUBACK	9	Subscribe Acknowledgment
UNSUBSCRIBE	10	Client Unsubscribe request
UNSUBACK	11	Unsubscribe Acknowledgment
PINGREQ	12	PING Request
PINGRESP	13	PING Response
DISCONNECT	14	Client is Disconnecting
Reserved	15	Reserved

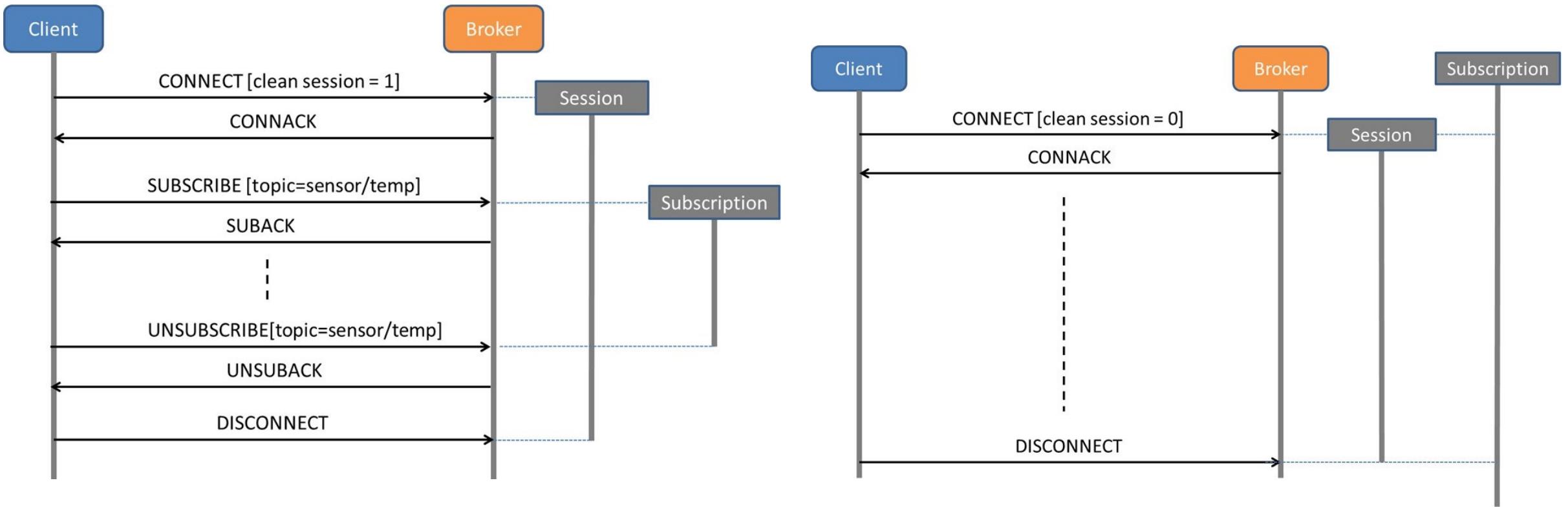
MQTT: format zaglavlja

Zaglavljje,
2 byte

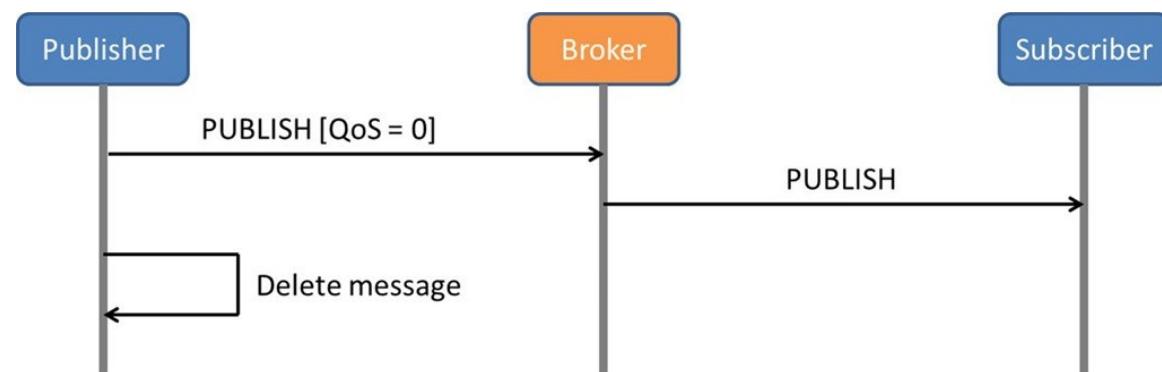
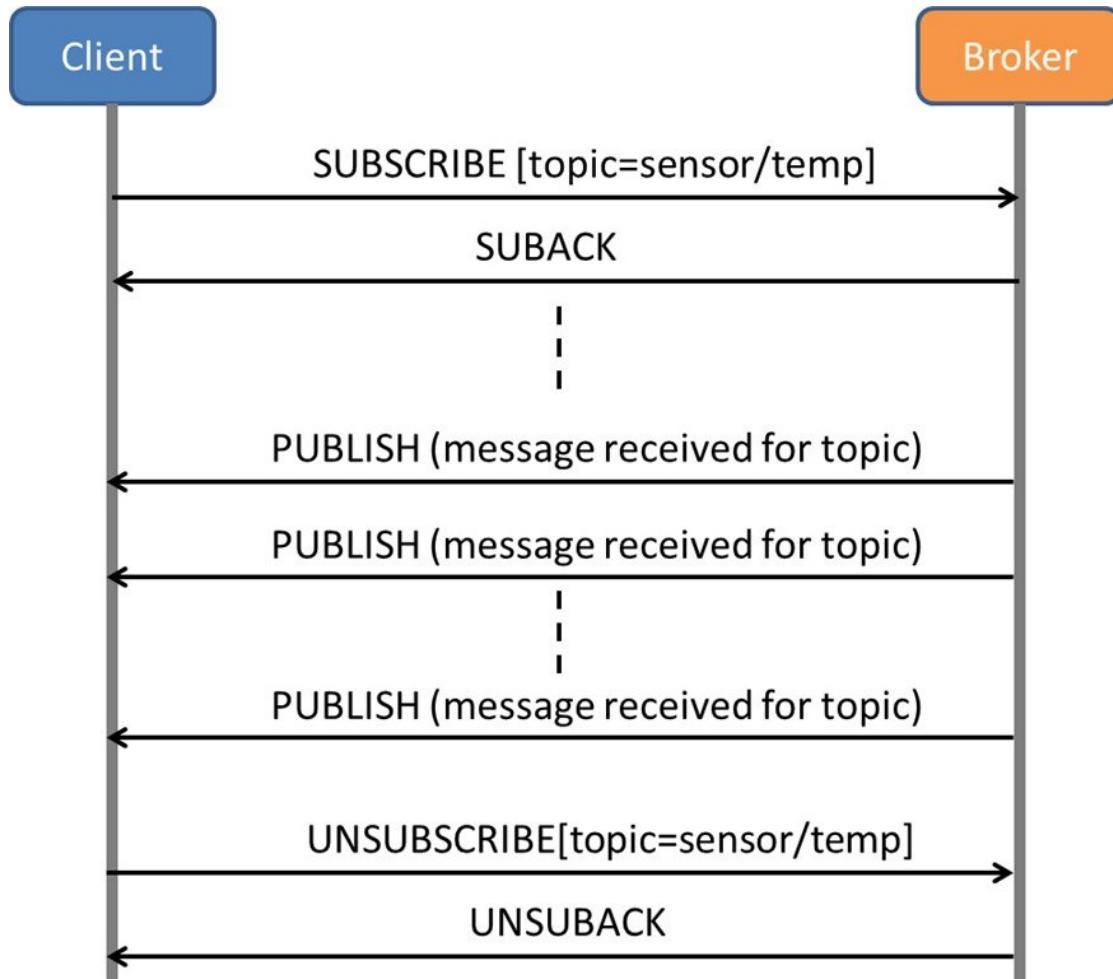
bit	7	6	5	4	3	2	1	0
byte 1					DUP flag		QoS level	RETAIN
byte 2						Remaining Length		

- **DUP flag** – ponovljeno slanje
- **QoS** – definira razinu kvalitete usluge (0, 1 ili 2)
- **RETAIN** – koristi se samo u porukama PUBLISH
 - Kada klijent šalje PUBLISH do brokera, ako je retain flag = 1, broker treba pohraniti poruku, poruka će biti isporučena novim pretplatnicima s odgovarajućom pretplatom (novi pretplatnici ne čekaju novu obavijest, već primaju posljednju poznatu vrijednost).
 - tzv. *retained messages*

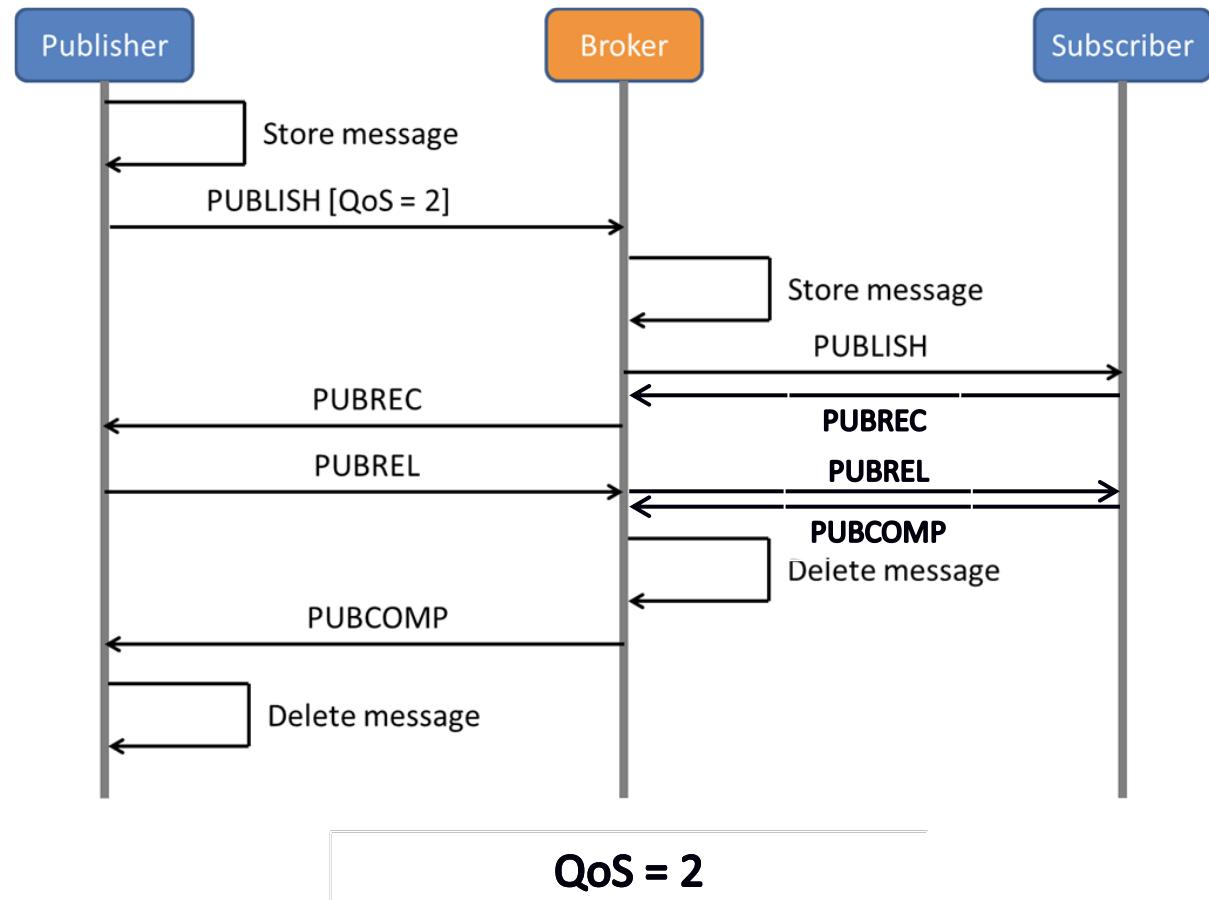
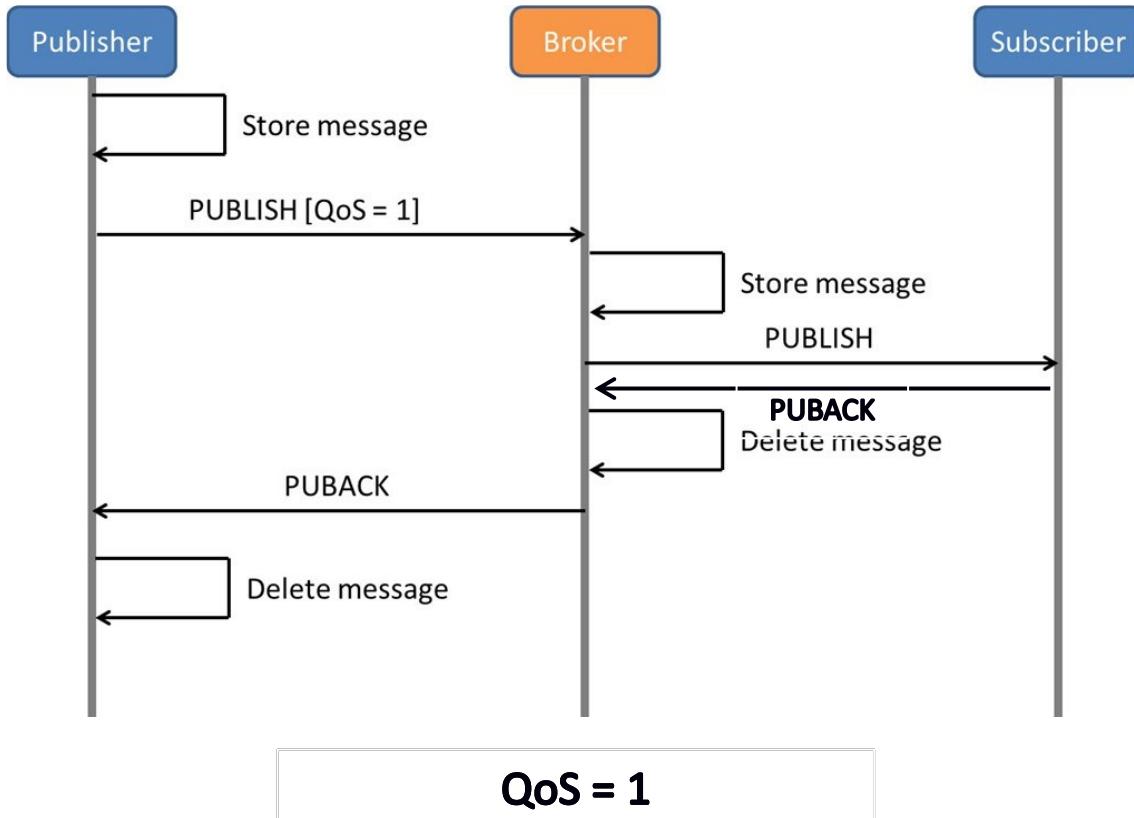
CONNECT/DISCONNECT



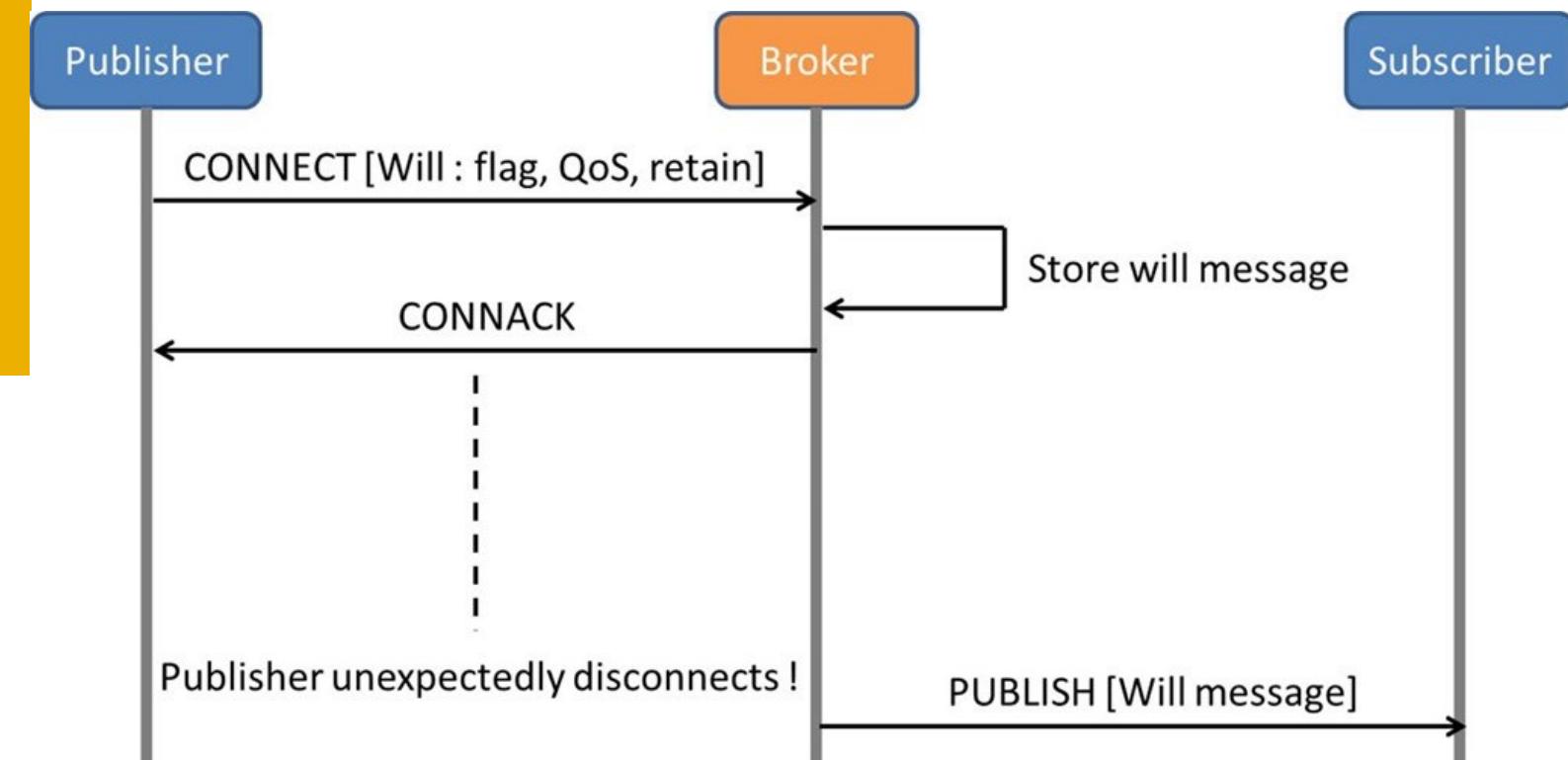
SUBSCRIBE/PUBLISH



PUBLISH, QoS>0



#Will message



- Publisher može prilikom stvaranja sjednice definirati *will flag*, *will topic* i *will payload*
- Ako dođe do njegovog nenadanog ispada, *will payload* se isporučuje preplatnicima

Prednosti i nedostaci MQTT-a

Prednosti

- Messaging protokol prilagođen uređajima i mrežama ograničenih resursa
- Pouzdana isporuka poruka (s obzirom da se temelji na TCP-u) u jednoj sjednici
- Preplata omogućuje isporuke poruke na više odredišta
- Različiti nivoi QoS-a: 1 i 2 osiguravaju isporuku poruke preplatnicima

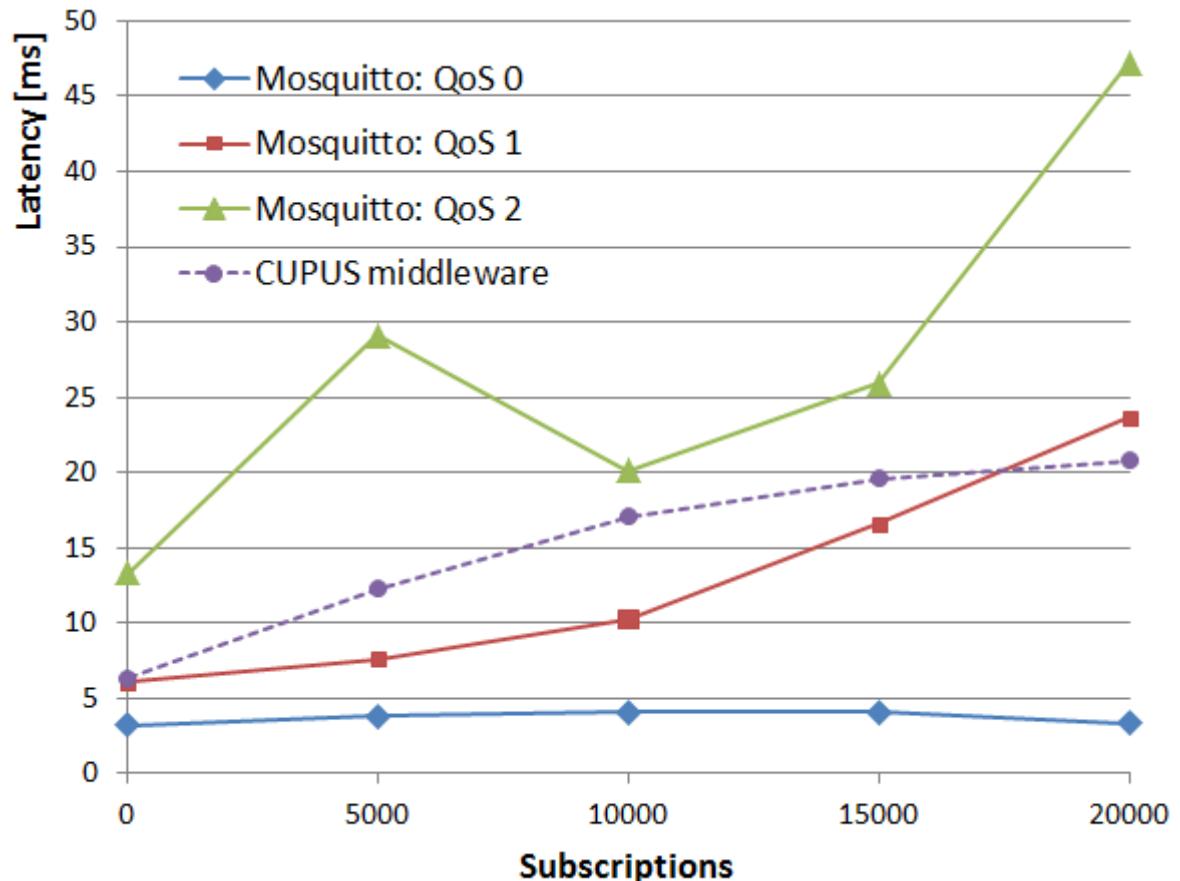
Nedostaci

- Korištenje TCP-a dodaje značajni overhead
 - Uređaj: podržava TCP/IP stack
 - Konekcija između klijenata i broker mora biti kontinuirano aktivna, čak i kada se ne šalju podaci ("keep alive")
- Značajna potrošnja energije na IoT-uređaju, nije pogodan za uređaje s ograničenom količinom energije
 - Postoji varijanta protokola koja se temelji na UDP-u, ali se rjeđe koristi

Usporedba CoAP-a i MQTT

	CoAP	MQTT
Communications Model	Request-Response, or Pub-Sub	Pub-Sub
RESTful	Yes	No
Transport Layer Protocol	Preferably UDP; TCP can be used	Preferably TCP; UDP can be used (MQTT-S)
Header	4 Bytes	2 Bytes
Number of message types	4	16
Messaging	Asynchronous and Synchronous	Asynchronous
Application Reliability	2 Levels	3 Levels
Security	IPSEC or DTLS	TLS
Intermediaries	Yes	Yes (MQTT-S)

Test performanci za MQTT



Usporedba vremena obrade i isporuke
poruka svim preplatnicima za QoS = 0, 1 i 2

MQTT server: Mosquitto
MQTT client: Paho

Izvor: Antonić, Aleksandar; Marjanović, Martina; Skočir, Pavle; Podnar Žarko, Ivana.

Comparison of the CUPUS middleware and MQTT protocol for smart city services // Proceedings of the 13th International Conference on Telecommunications / Plank, Thomas (ur.).

Graz : Graz University of Technology, 2015. 1-8

Literatura

1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, and Jerome Henry. 2017. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things (1st ed.). Cisco Press. (6. poglavlje)
2. MQTT Version 5.0, <https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html>



SVEUČILIŠTE U ZAGREBU



Diplomski studij

Računarstvo

Znanost o mrežama

Programsko inženjerstvo i informacijski
sistemi

Računalno inženjerstvo

Informacijska i komunikacijska tehnologija

Automatika i robotika

Informacijsko i komunikacijsko inženjerstvo

Elektrotehnika i informacijska tehnologija

Audiotehnologije i elektroakustika

Elektroenergetika

(Izborni predmet profila)

Internet stvari

5. Komunikacijski protokoli za
komunikaciju uređaja (sloj podatkovne
poveznice): LoRaWAN, LTE-M, NB-IoT

Ak. god. 2022./2023.

Sadržaj

- Sigfox
- LoRa i LoRaWAN
- LTE-M
- NB-IoT

LPWAN – Low Power Wide Area Network

- Mala potrošnja energije
- Uređaji mogu raditi na bateriju
- Velike udaljenosti komunikacije (~x km)
- Niže frekvencije komunikacije → povećana udaljenost
- Manja brzina prijenosa podataka

Sigfox



- Tehnologija razvijena 2009. u Toulouse, France
- Patentirana i zatvorena tehnologija
- Koristi nelicencirani pojas ISM
- Ograničenja:
 - Do 140 poruka po uređaju dnevno može poslati (*duty cycle 1%, 6 poruka/sat*)
 - Veličina podataka koje prenosi: 12 okteta (slanje) i 8 okteta (primanje)
 - Brzina prijenosa do 100 bps (slanje) i 600 bps (primanje)
- Originalno je zamišljen da je komunikacija ide u jednom smjeru (kao senzorska mreža)

Sigfox – fizički sloj



- Ultra Narrow Band (UNB)
- Frekvencije:
 - 868 MHz: Europa (regulatorni dokument ETSI 300-200)
 - 902 MHz: Sjeverna Amerika (regulatorni dokument FCC part 15)
- 333 kanala, širina kanala 100 Hz
- Osjetljivost prijamnika: -120 dBm/-142 dBm
- Snaga predajnika: +14 dBm, a u Sjevernoj Americi +22 dBm

Sigfox – sloj podatkovne poveznice



- MAC – okvir kod slanja (*uplink*)

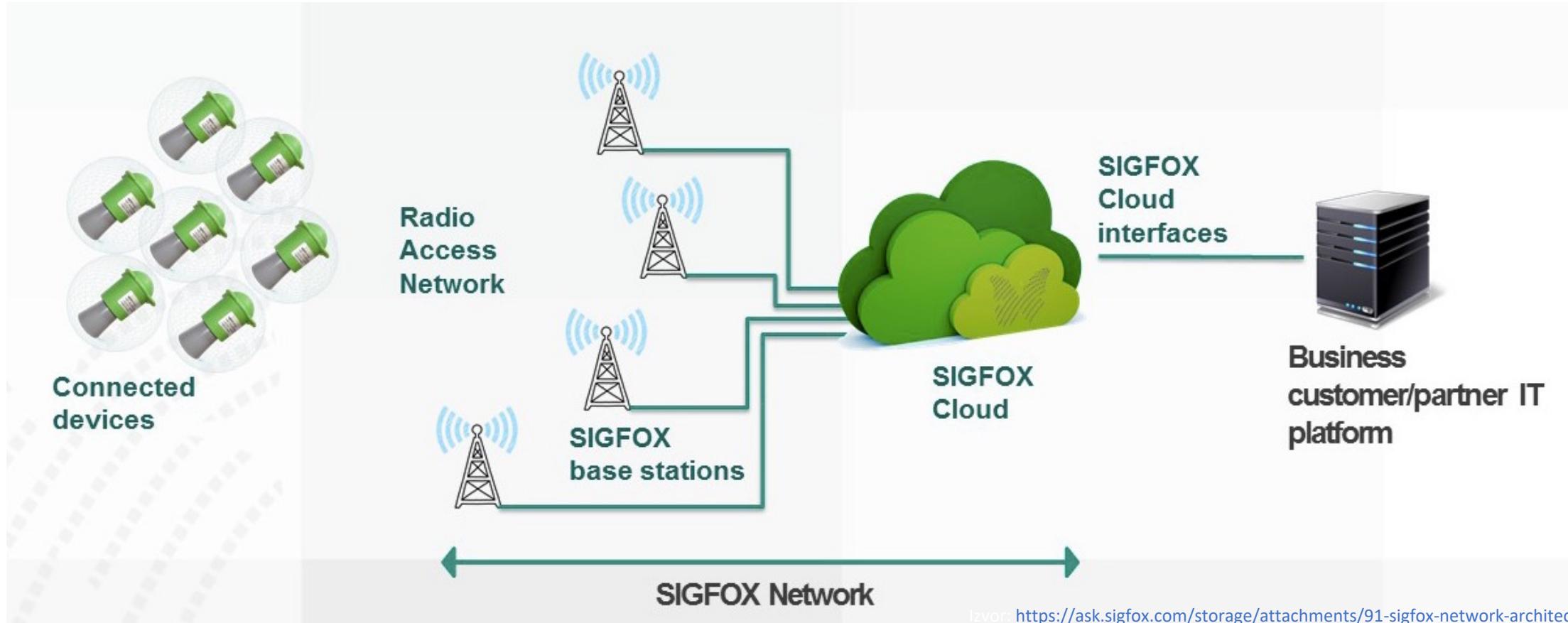
32 bita	16 bita	32 bita	0-96 bitova	varijabilno	16 bita
Preambula	Sink. okvira	ID krajnjeg uređaja	Sadržaj okvira	Autentikacija	FCS

- MAC – okvir kod primanja (*downlink*)

32 bita	13 bita	2 bita	8 bita	16 bita	varijabilno	0-64 bita
Preambula	Sink. okvira	Zastavice	FCS	Autentikacija	Kodovi greške	Sadržaj okvira

- FCS – Frame Check Sequence

Sigfox – topologija



Sigfox – primjena



- Za slanje male količine podataka u praskovima (*burst*)
- Alarmi
- Jednostavna brojila
- Senzori okoline (ne velike preciznosti ~0,004)

LoRa i LoRaWAN

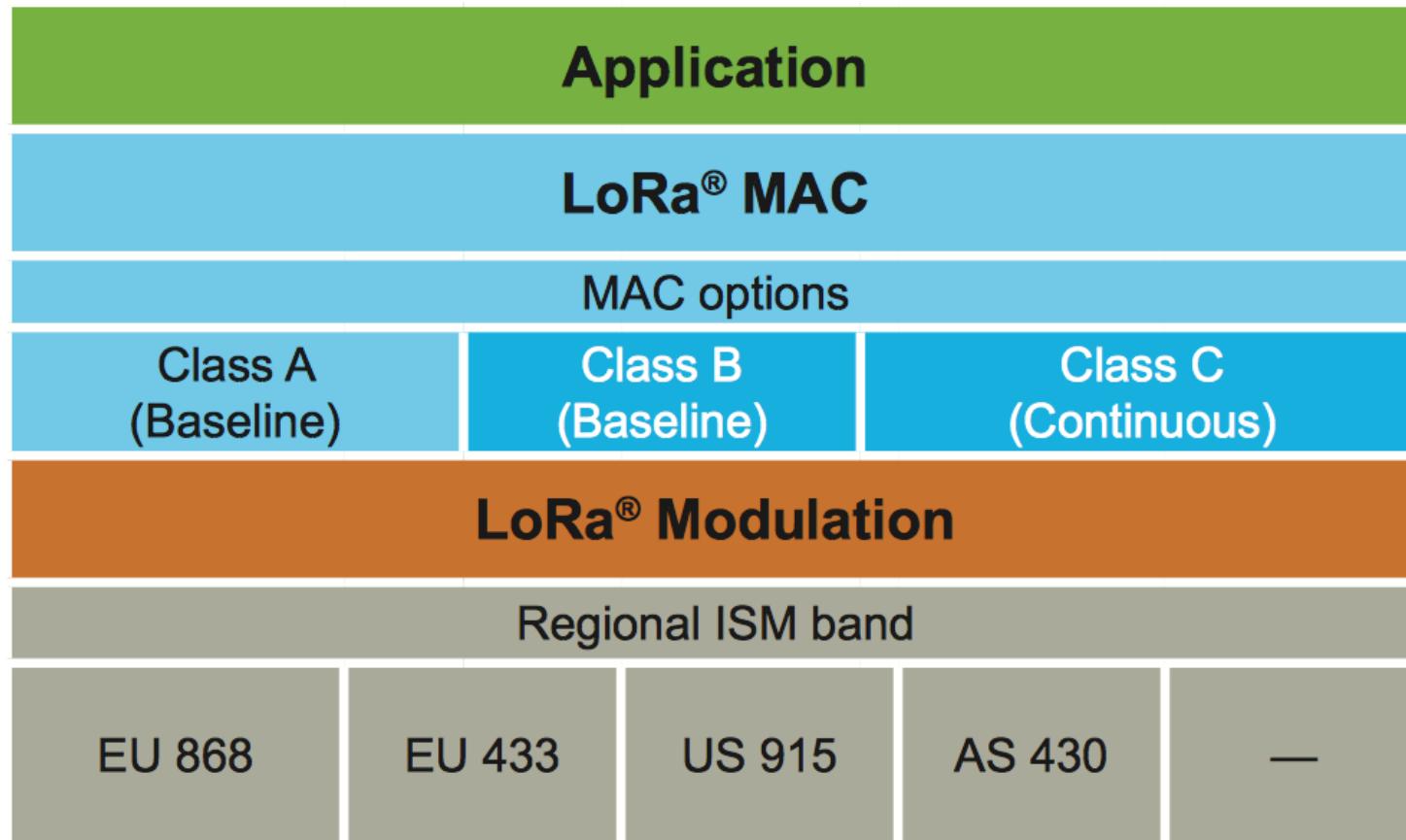


LoRa ili LoRaWAN



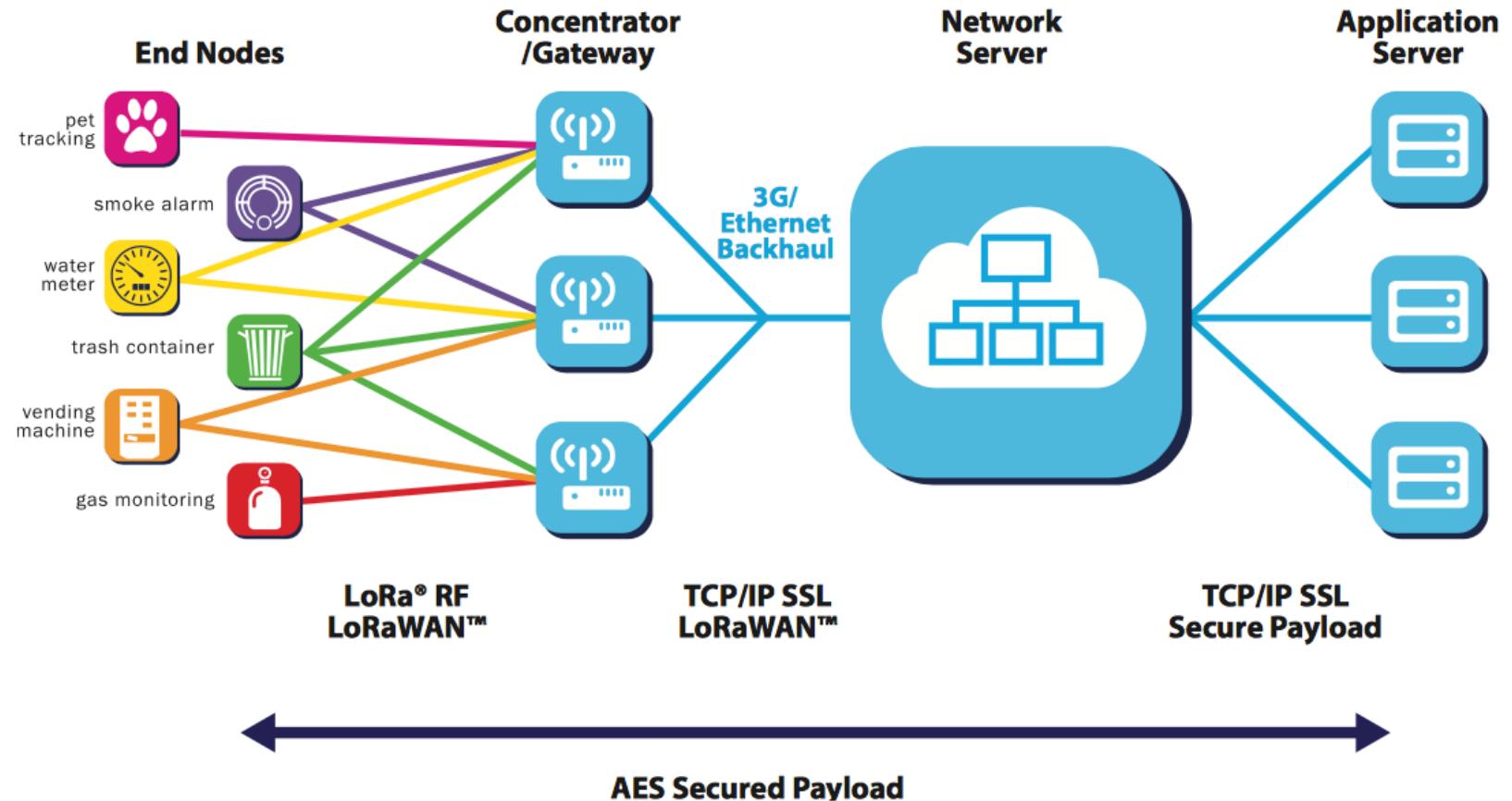
- LoRa – definira fizički sloj
- LoRaWAN – definira protokol i arhitekturu sustava

LoRa – arhitektura čvora



https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

LoRa – mrežna arhitektura

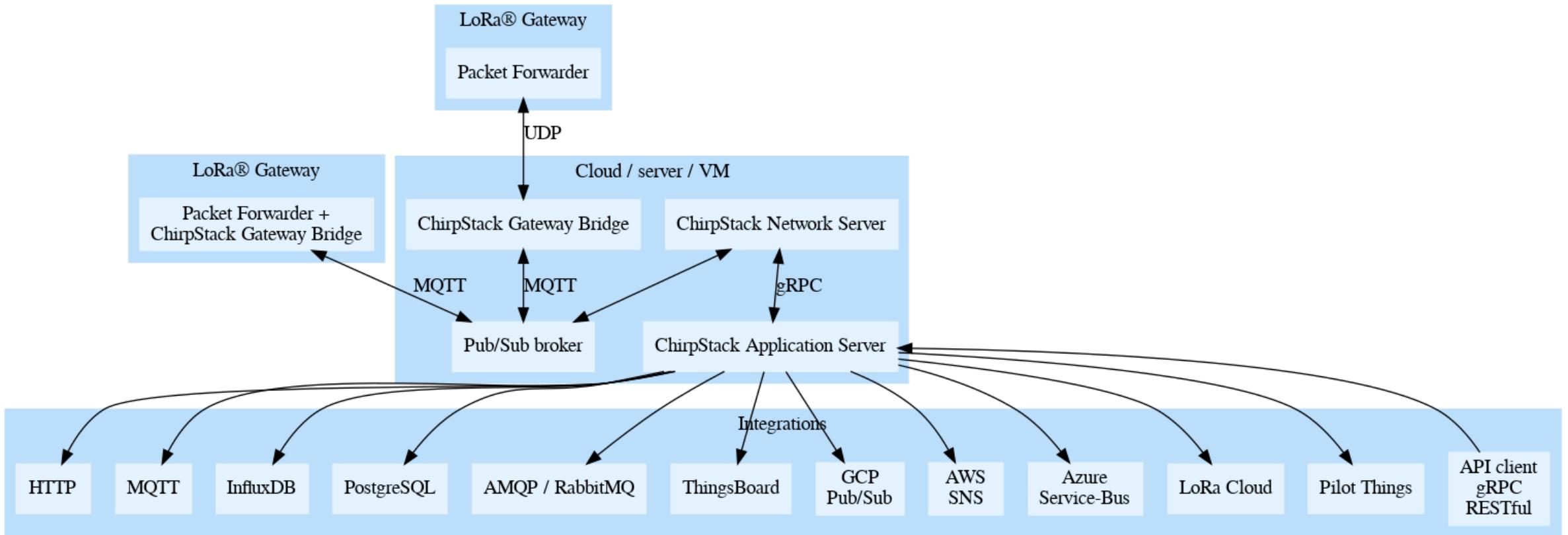


https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

ChirpStack

- LoRaWAN Network Server složaj otvorenog koda
- komponente:
 - ChirpStack Gateway Bridge
 - za komunikaciju s mrežnim prilazom
 - ChirpStack Network Server
 - implementacija mrežnog poslužitelja
 - ChirpStack Application Server
 - implementacija aplikacijskog poslužitelja
 - ChirpStack Gateway OS
 - za izvođenje cijelog složaja na mrežnom prilazu koji je na Raspberry Pi-u
 - temelji se na Linuxu

ChirpStack - arhitektura



LoRa – klase uređaja



- Klasa A
 - Najbolje za napajanje baterijama
 - Svi uređaji u mreži podržavaju ovaj način rada
 - Slanje podataka na uređaj je moguće samo nakon uspješnog slanja
 - Koristi se mehanizam ALOHA
- Klasa B
 - Primanje u raspoređenom vremenskom periodu
 - Prima signal za sinkronizaciju od GW-a
- Klasa C
 - Kontinuirano ima otvoren prozor za primanje
 - Primanje se zaustavlja jedino kada se šalju podaci

Frekvencije rada



	Europe	North America	China	Korea	Japan	India
Frequency band	867-869MHz	902-928MHz	470-510MHz	920-925MHz	920-925MHz	865-867MHz
Channels	10	64 + 8 + 8				
Channel BW Up	125/250kHz	125/500kHz				
Channel BW Dn	125kHz	500kHz				
TX Power Up	+14dBm	+20dBm typ (+30dBm allowed)				
TX Power Dn	+14dBm	+27dBm				
SF Up	7-12	7-10				
Data rate	250bps- 50kbps	980bps-21.9kbps				
Link Budget Up	155dB	154dB				
Link Budget Dn	155dB	157dB				

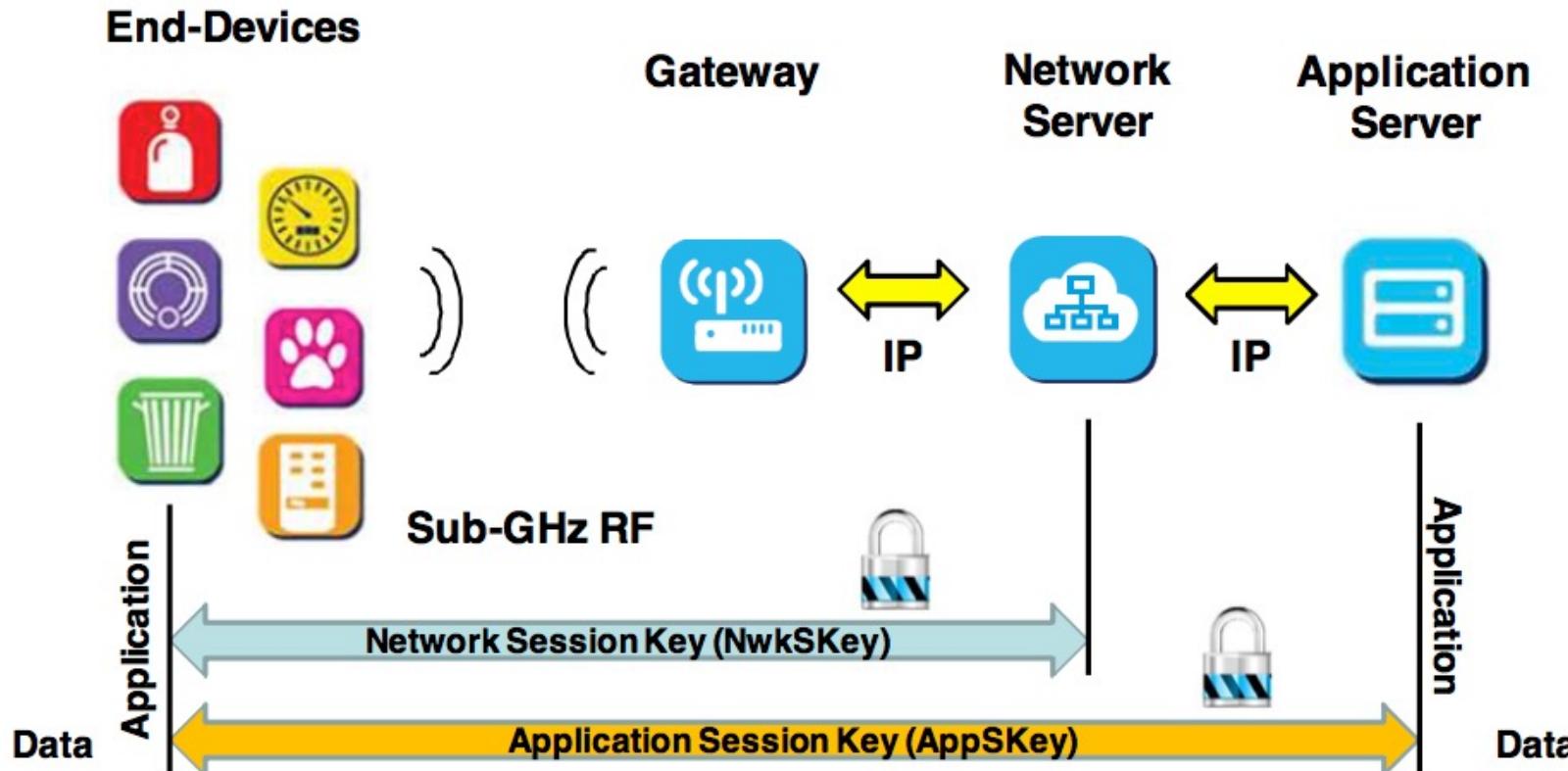
In definition by Technical Committee

<http://www.3glteinfo.com/lora/lorawan-frequency-bands/>

Sigurnost



- Koristi se AES-128 kao i u IEEE 802.15.4



Aktivacija



- Prije nego se krajnji uređaj može koristiti u mreži LoRaWAN potrebno ga je aktivirati
- Informacije potrebne za aktivaciju su:
 - Adresa uređaja – Device Address (DevAddr)
 - 32 bita, jedinstven u mreži, šalje se u svakom okviru
 - Koriste ga: krajnji uređaj, mrežni poslužitelj i aplikacijski poslužitelj
 - Ključ mrežne sjednice – Network Session Key (NwkSKey)
 - Ključ od 128 bita – AES, jedinstven za svaki krajnji uređaj, omogućuje integritet komunikacije
 - Koriste ga: krajnji uređaj i mrežni poslužitelj
 - Ključ aplikacijske sjednice – Application Session Key (AppSKey)
 - Ključ od 128 bita – AES, jedinstven za svaki krajnji uređaj, koristi se zaštitu aplikacijskih podataka
 - Koriste ga: krajnji uređaj i aplikacijski poslužitelj

Aktivacija



- Dvije aktivacijske metode:
 1. Over-the-Air Activation (OTA A)
 - Temelji se na globalno jedinstvenom identifikatoru
 - Poruke se razmjenjuju bežično
 2. Activation By Personalization (ABP)
 - Dijeljeni ključevi se pohranjuju na krajnji uređaj u proizvodnji
 - Vrijede samo za specifičnu mrežu

http://www.chipcad.hu/letoltes/19065_IoT4_FinalSlides.pdf

Implementacije

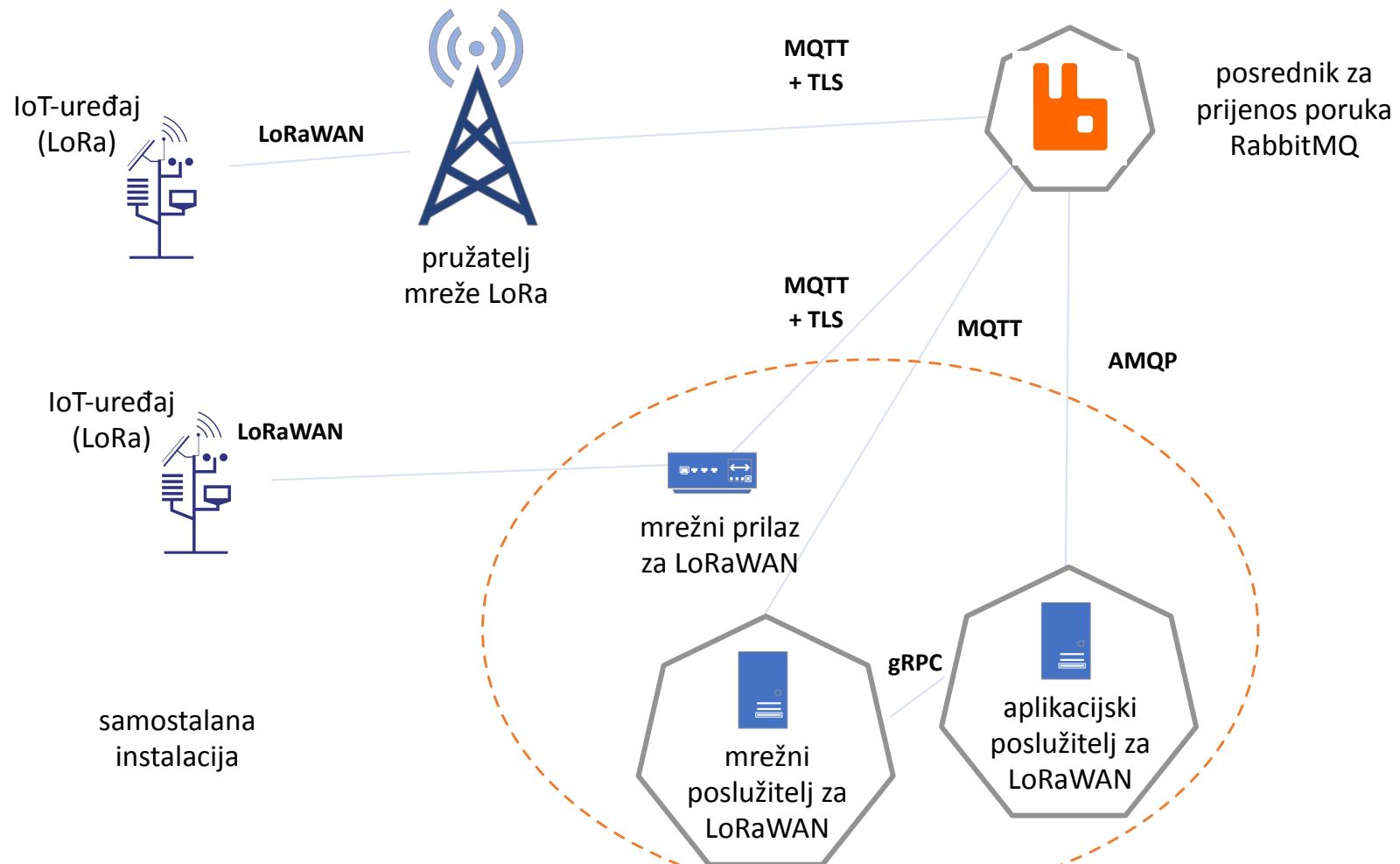


- Komercijalne:
 - Operatori pružaju mrežu i naplaćuju ju:
 - OiV (Hrvatska), KPN (Nizozemska), Orange (Francuska), Unidata (Italija), ...
 - Unidata (partner na projektu symbIoTe) - operator LoRaWAN mreže u Italiji
 - <https://www.i-scoop.eu/internet-of-things-guide/iot-network-lora-lorawan/>
 - Javne:
 - Bilo tko se može uključiti i pružati pristup
 - Ažurni popis na <https://www.thethingsnetwork.org>
 - Privatne:
 - Svatko može pokrenuti svoju privatnu mrežu

Implementacija LoRaWAN-a u IoT labu



IoT-polje





Projekti i studentski radovi s LoRaWAN-om

M2M Communications Challenges



- U suradnji s kompanijom Ericsson Nikola Tesla
- Od 2011. - svake godine druga tema
- Teme vezane uz Machine-to-Machine (M2M) komunikaciju
- 2017.
 - Uporedba LoRaWAN-a s NB-IoT-om, BLE, WiFi
 - Izrada prototipa s više tehnologija na jednom krajnjem uređaju
 - Odabir komunikacijske tehnologije ovisno o kontekstu

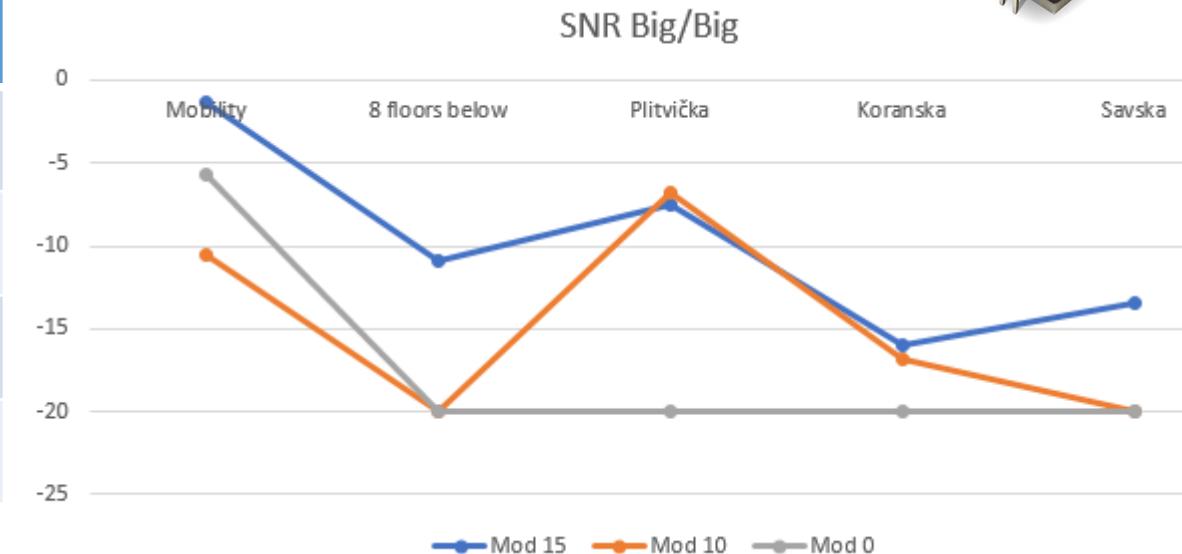
Mjerenje vanjskih prilika te praćenje potrošnje energije LoRa i LoRaWAN modula

- Studentski projekt na diplomskom studiju
 - Mateo Červar, Matija Cvetnić



Potrošnja energije koristeći *small* i *big* antene [mA]

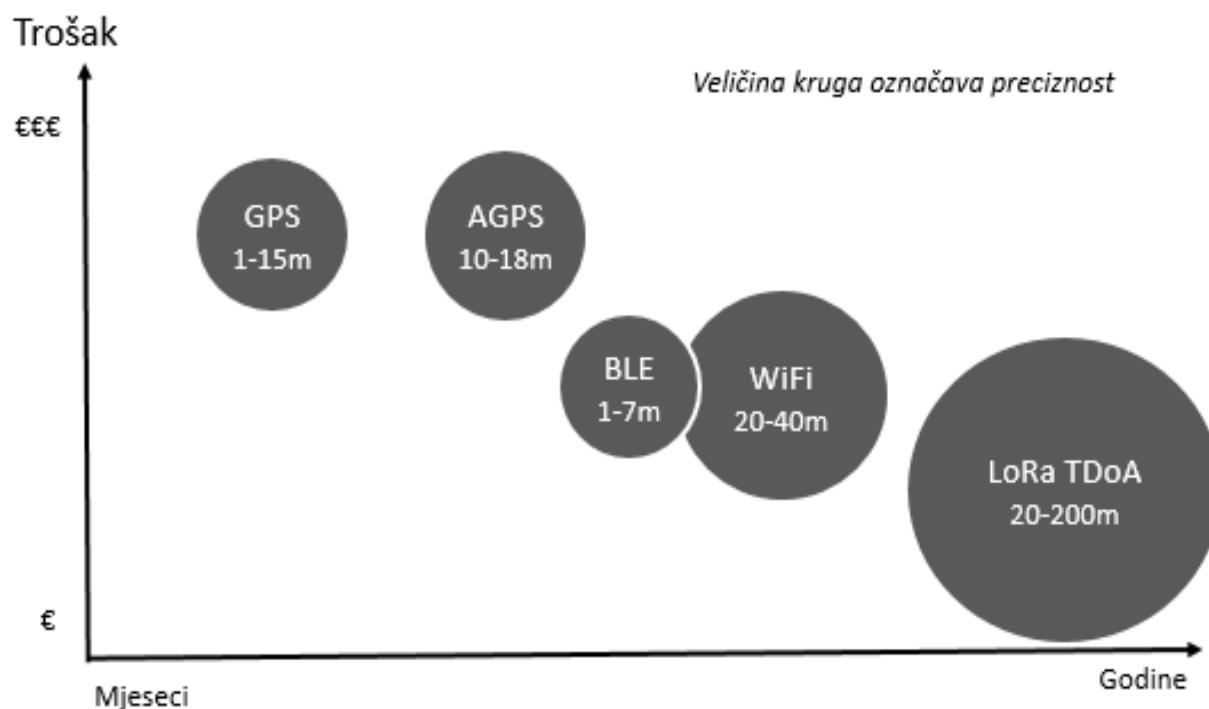
	Antenna size	Low (0)	High (10)	Max (15)
LoRa	Small	19.7	22.96	39.4
	Big	19.86	23.2	40.8
LoRaWAN	Small	17.74	32.66	39.34
	Big	18.56	33.02	40.08



Lociranje uređaja u Internetu stvari (1)



- Diplomski rad:
Mateo Červar

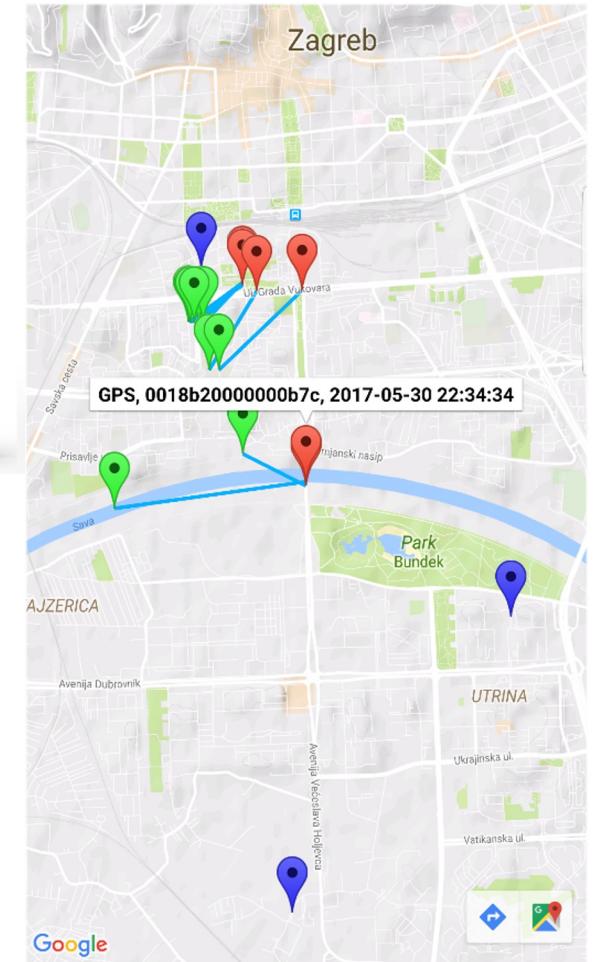
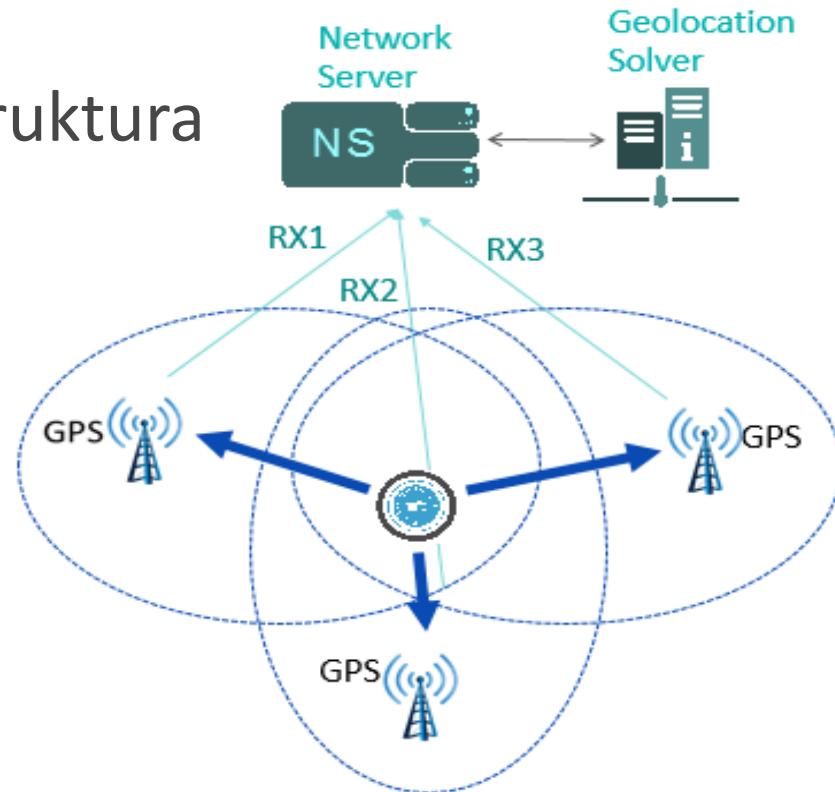


Usporedba tehnologija pozicioniranja

Lociranje uređaja u Internetu stvari (2)

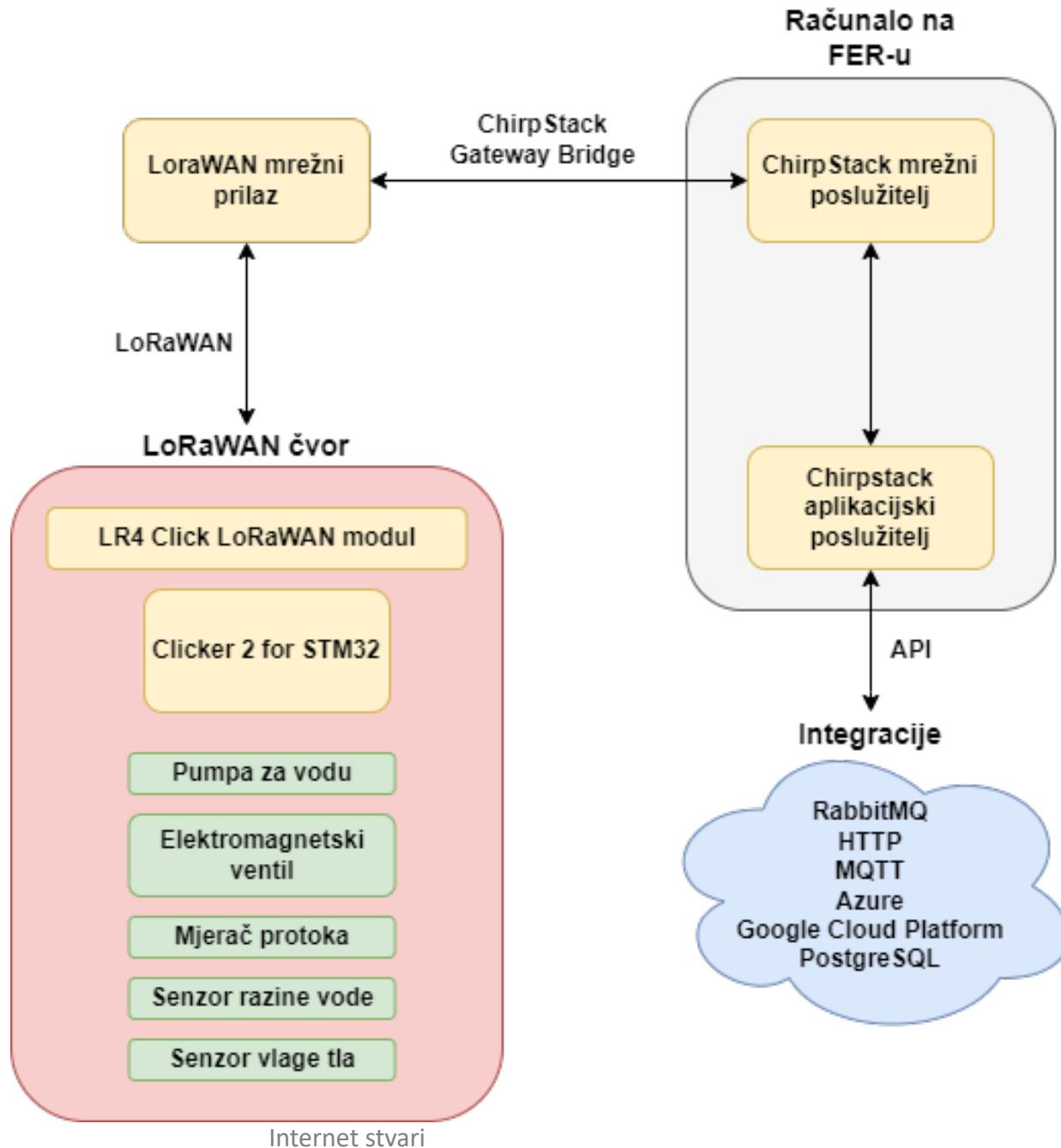
- Diplomski rad: Mateo Červar

- Mrežna infrastruktura

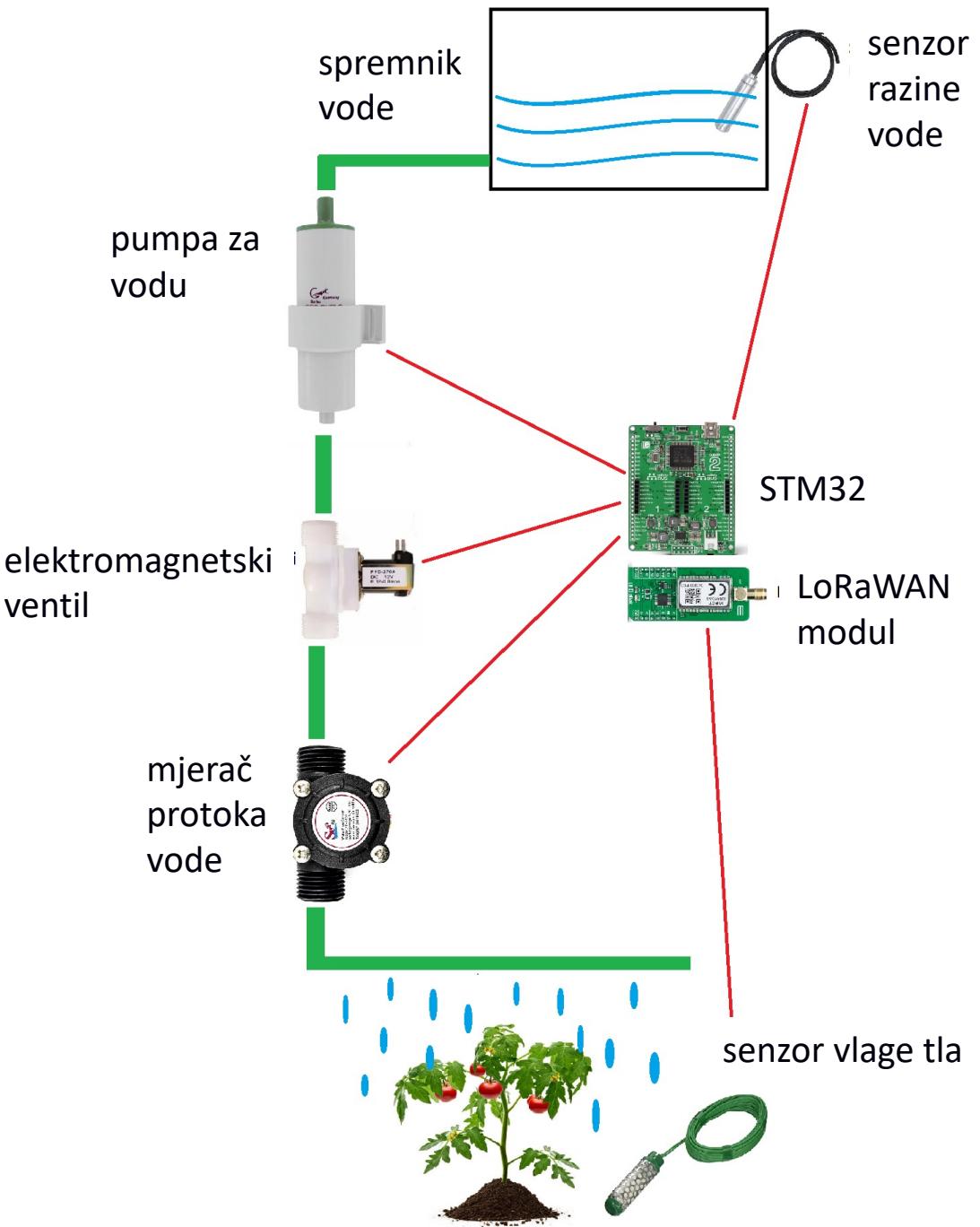
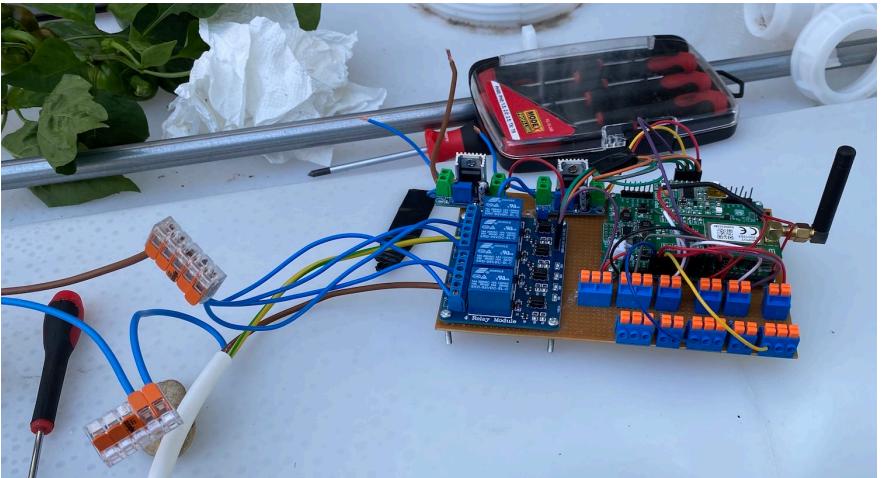


Prikupljanje podataka i aktuacija s uređajima u urbanom vrtu (1)

- Arhitektura



Prikupljanje podataka i aktuacija s uređajima u urbanom vrtu (2)



Pokretna mreža

Standardi i standardizacijska tijela

- ITU – International Telecommunication Union
 - Najviše definiraju ciljeve i standarde za uređaje koji će biti označeni sa 4G ili 5G
- 3GPP
 - Konzorcij koji definira tehnologije i nadogradnje
 - Sve je organizirano u izdanja (release):
 - Rel 8-9: LTE (2008., 2009.)
 - Rel 10-12: LTE Advanced (2011., 2012., 2015.)
 - Rel 12: **LTE-M (Cat 0)**
 - Rel 13-14: LTE Advanced Pro (2016., 2017.)
 - Rel 13: **LTE Cat-M1 (eMTC), NB-IoT (LTE Cat-NB ili NB1)**
 - Rel 14: Vehicle-to-Everything (V2X), poboljšanja za MTC, NB-IoT (NB2)
 - Rel 15: (2019.) – poboljšanja za MTC, 5G Vehicle-to-x service (V2X)
 - Rel 16: (2020.) – 5G expansion (advanced V2X, Industrial IoT, URLLC), 5G Efficiency (power consumption)

LTE-M

LTE Cat 0 – Release 12

- Smanjene brzine prijenosa na 1Mbps
- Half-duplex komunikacija
- Uveden Power Save Mode (PSM)
 - Uredjaj može ući u duboki san i brzo se probuditi i povezati
 - Može se jednom dnevno buditi i slati podatke
 - Maksimalni period spavanja 12.1 dana (ovisi o mreži npr. 2 ili 4 sata)

LTE Cat-1 – Release 8

- Prvenstveno se koristi u SAD-u za M2M komunikaciju
- Veće brzine: 10Mbps (skidanje), 5Mbps (slanje)
- Može prenositi zvuk i video
- Manja potrošnja energije nego 4G-LTE
- Može se prebaciti na 3G ili 2G

LTE Cat-M1 (eMTC ili LTE-M) – Release 13

- eMTC – enhanced Machine Type Communication
- Smanjena širina pojasa sa 20MHz na 1,4Mhz → jednostavniji uređaji, manja potrošnja
- Smanjena izlazna snaga za 50%
- Brzine 375 Kbps ili 1 Mbps
- Primjena: V2V, zvuk
- Dodani mehanizmi za mogućnost kratkog spavanja uređaja (10,24s) → radio troši 15µA u prosjeku
- PSM iz Cat-0 se primjenjuje i ovdje

NB-IoT

NB-IoT (LTE Cat-NB ili NB1) – Release 13

- Ciljevi:
 - 10 godina trajanja baterija s kapacitetom 5 Wh
 - Dodatna pokrivenost prostora (+20 dB)
 - Cijena modula ~\$5
- Bitne promjene:
 - Širina kanala samo 180kHz → smanjenje troškova modula i potrošnje energije
 - Nema prijenosa zvuka ili videa
 - Nema pokretnosti između ćelija
 - Maksimalni gubitak signala (MCL – max. coupling loss) 164 dB što je slično LoRaWAN-u i Sigfoxu
 - Komunikacija prolazi u podrumima, tunelima
 - Povećan domet za 7x na otvorenom prostoru
- Brzina prijenosa: ~26Kbps *downlink*, ~62Kbps *uplink*

NB-IoT – smještaj kanala

- Između dva LTE kanala
 - U praznom dijelu koji nije iskorišten
- Na mjestu GSM kanala
 - Neki GSM kanali se onda koriste za NB-IoT
- Unutar LTE kanala
 - Multipleksiranje LTE-a i NB-a
- Teoretski omogućuje spajanje do 200.000 uređaja po ćeliji

NB-IoT (NB2) – Release 14

- Glavne nadogradnje:
 - preciznije pozicioniranje: OTDOA i E-CID
 - dodano višeodredišno razašiljanje (*multicast*)
 - poboljšana mobilnost
 - moguće ponovno spajanje kada smo spojeni, nije potrebno ići u mod rada *idle*
 - povećane maksimalne brzine:
 - 127Kbps *downlink*, 159Kbps *uplink*
 - podrška za više (15) operatora (uz matičnog) → povećana gustoća uređaja $1\text{M}/\text{km}^2$
 - Nova klasa snage 14dBm → potrebne manje baterije

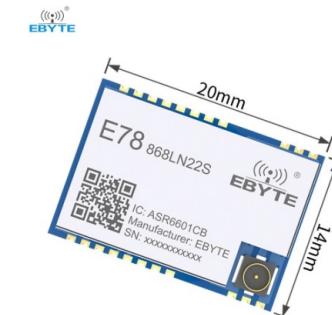
NB-IoT – prve instalacije 2017.

- DT – pokrenuto u 8 zemalja u EU (Njemačka, Nizozemska, Austrija, Hrvatska, Grčka, Mađarska, Poljska, Slovačka)
 - Primjene: praćenje stvari, pametno parkiranje, pametna brojila
- T-Mobile US, Ericsson, Qualcomm
 - Primjene: prikupljanje senzorskih podataka (temp., vlažnost, plinovi, ...), alarmiranje za poplave
- U-blox, PinMyPet, Huawei i operator Vivo: praćenje životinja
- China Mobile, ZTE – testiranje mreže na 200 mjesta
- Telia Norway – pilot projekt za praćenje 1000 ovaca u Norveškoj

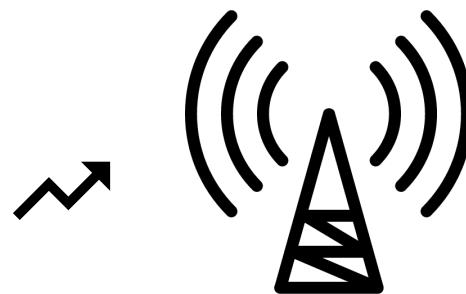
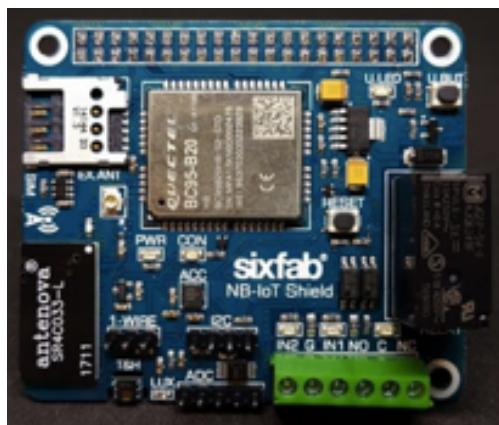
NB-IoT moduli



- sixfab – [Arduino NB-IoT Shield](#) (80€ → 62€), [Raspberry Pi NB-IoT Shield](#) (80€)
 - Ovo imamo u laboratoriju
- [QUECTEL BG96 LTE CAT M1/CAT NB1/EGPRS](#) - ~30€
- [Dragino](#) - ~45\$ → 20€
- Botletics SIM7000 LTE CAT-M1 NB-IoT Cellular - ~125\$ → 65\$
- ASR6601 LoRaWAN 868MHz SoC LoRa RF IoT Wireless Module Long Range Data Transceiver Development Board E78-868LN22S(6601) Ebyte – [AlliExpress](#) 8\$
- SIMCom SIM7070G – [AlliExpress](#) ~17€



NB-IoT arhitektura sustava

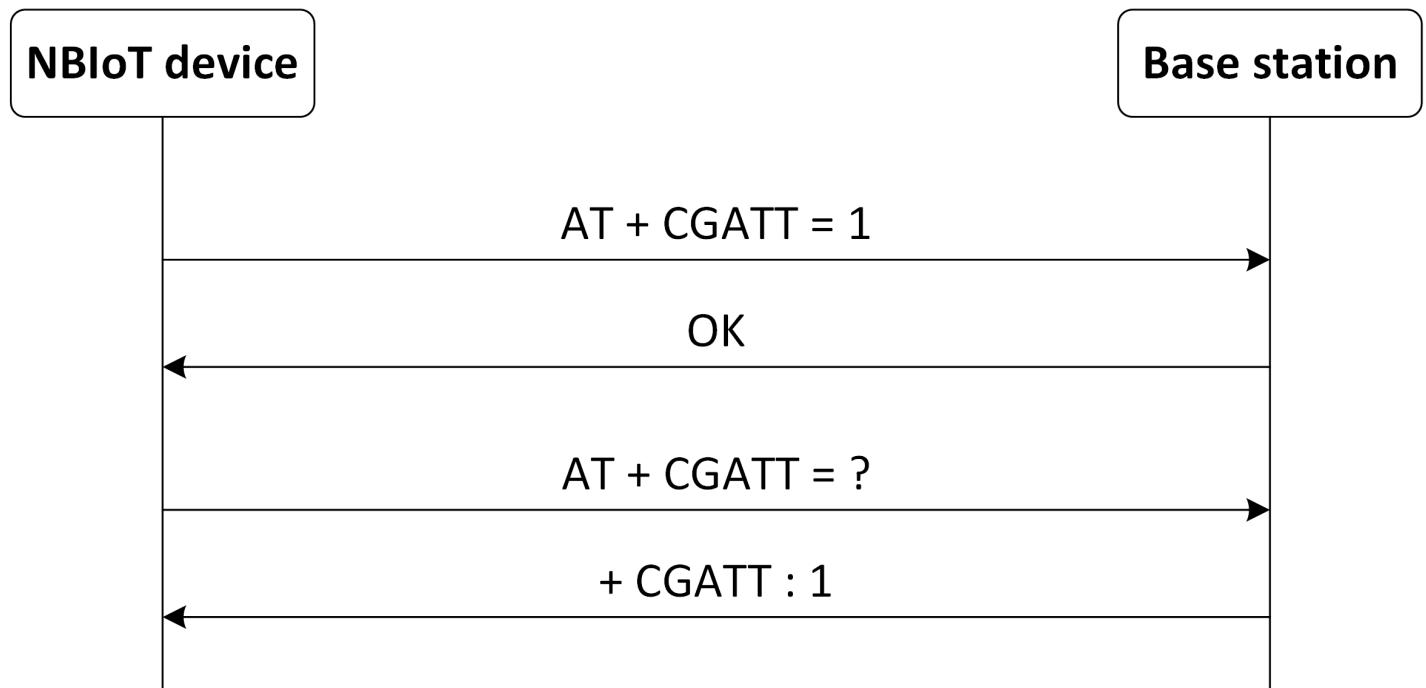


Spajanje na mrežu

- Koriste se AT komande za komunikaciju s modulom

- CGATT – spajanje/odspajanje na/sa mrežu/e

- Format:
 - $AT+CGATT=<state>$
- State:
 - 0 – odspajanje
 - 1 – spajanje



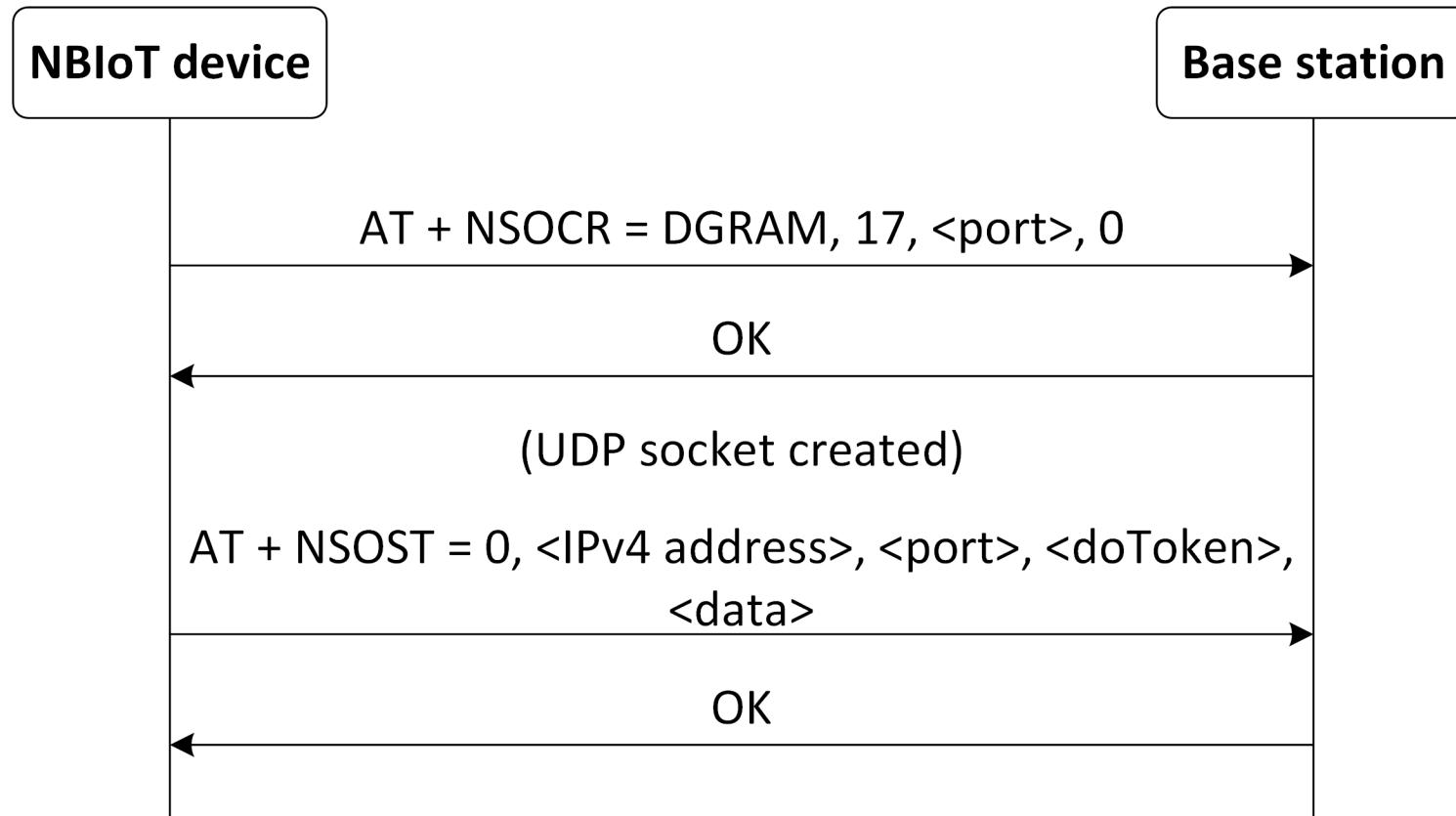
Kreiranje socketa

- AT+NSOCR – kreiranje socketa
 - Format: AT+NSOCR=<type>,<protocol>,<listen port>[,<receive control>]
 - Type – dozvoljeno jedino DGRAM
 - Protocol – broj protokola ([vidi](#)), za UDP je 17
 - Listen port – lokalna vrata na kojima sluša (0-65535)
 - Receive control
 - 1 – treba primiti odgovor (podrazumijevano)
 - 0 – ne treba odgovor
 - AT+NSOST - slanje paketa
 - Format: AT+NSOST=<socket>,<remote_addr> ,<remote_port>, <length>,<data>
 - Socket – broj vraćen u komandi AT+NSOCR

Slanje UDP paketa

- AT+NSOST - slanje paketa
 - Format: AT+NSOST=<socket>,<remote_addr> ,<remote_port>, <length>,<data>
 - Socket – broj vraćen u komandi AT+NSOCR
 - Remote addr - IPv4 u notaciji s točkom (decimalno, oktalno ili hex)
 - Remote port – vrata na koja se šalje
 - Length – dužina u oktetima (max 512)
 - Data – podaci u HEX obliku
 - Primjer:
 - AT+NSOST=0,192.158.5.1,1024,2,AB30
 - Odgovor:
 - <socket>,<length>
 - OK

Dijagram kreiranja socketa i slanja



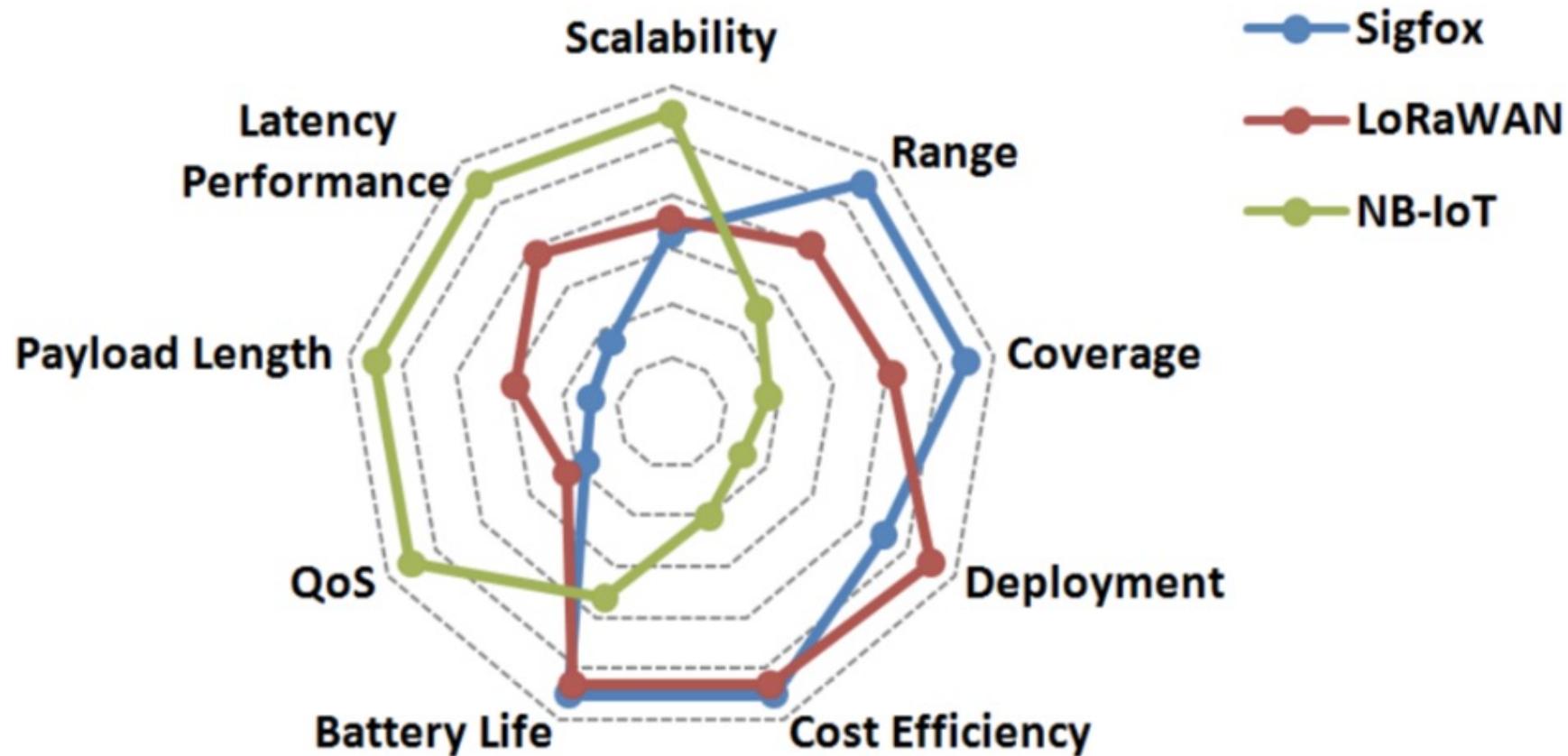
Primanje UDP paketa

- AT+NSORF – primanje UDP paketa
 - Format: AT+NSORF=<socket>,<req_length>
 - Socket – socket iz odgovora AT+NSOCR
 - Req length – max broj podataka koji će biti vraćen u broju okteta
 - Format odgovora: <socket>,<ip_addr>,<port>,<length>,<data>,<remaining_length>
 - Socket – socket
 - IP addr – adresa pošiljatelja
 - Length – dužina podataka
 - Data – podaci u hex stringu
 - Remaining length – količina podataka koje se može još pročitati za ovu poruku

Primjer komande:
AT+NSORF=0,10

Odgovor:
0,192.168.5.1,1024,2,ABAB,0
OK

Usporedba tehnologija



https://www.researchgate.net/publication/323907156_Overview_of_Cellular_LPWAN_Technologies_for_IoT_Deployment_Sigfox_LoRaWAN_and_NB-IoT

Pitanja za ponavljanje

- Koja su osnovna svojstva LPWAN-a?
- Čemu služi Sigfox?
- Koliko se dnevno podatka može poslati pomoću Sigfoxa?
- Kakav je poslovni model Sigfoxa?
- Koja je razlika između tehnologija LoRa i LoRaWAN?
- Od koja 4 elementa se sastoji mrežna arhitektura LoRae?
- Objasnite razliku između 3 klase LoRa uređaja.
- Objasnite 2 načina aktivacije uređaja u LoRai.
- Čemu služi LTE-M?
- Koja je razlika između: LTE Cat-0, LTE Cat-1 i LTE Cat-M1?
- Koja su svojstva LTE Cat-M1?
- Što je NB-IoT i koja su mu svojstva?
- Kako se može smjestiti NB-IoT kanal?
- O čemu ovisi odabir neke tehnologije za neko IoT rješenje?



SVEUČILIŠTE U ZAGREBU



Internet stvari

Diplomski studij

Računarstvo

Znanost o mrežama

Programsko inženjerstvo i informacijski
sistemi

Računalno inženjerstvo

Informacijska i komunikacijska tehnologija

Automatika i robotika

Informacijsko i komunikacijsko inženjerstvo

Elektrotehnika i informacijska tehnologija

Audiotehnologije i elektroakustika

Elektroenergetika

(Izborni predmet profila)

**6. Protokoli za optimizaciju mrežnog
sloja: 6LoWPAN, 6TiSCH i RPL**

Ak. god. 2022./2023.

Sadržaj

- Uređaji i mreže ograničenih resursa
- 6LoWPAN: IPv6 over Low Power Wireless Personal Area Networks
- 6TiSCH: IPv6 over the TSCH mode of IEEE 802.15.4e
- RPL: IPv6 Routing Protocol for Low Power and Lossy Networks

Uređaji ograničenih resursa

Specificirani u RFC 7228

Uređaji s ograničenom memorijom, procesorom, napajanjem: smanjena sposobnost obrade podataka, mala veličina okvira pri prijenosu podataka

Uređaji kategorije 0 imaju izrazito ograničene resurse, ne implementiraju IP stack i sigurnosne mehanizme

Uređaji kategorije 1 ne implementiraju IP stack u cijelosti, podržavaju CoAP

Uređaji kategorije 2 implementiraju IP stack u cijelosti

Class	Definition
Class 0	This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms. An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging new unlicensed LPWA wireless technology.
Class 1	While greater than Class 0, the processing and code space characteristics (approximately 10 KB RAM and approximately 100 KB Flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP). This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.
Class 2	Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.

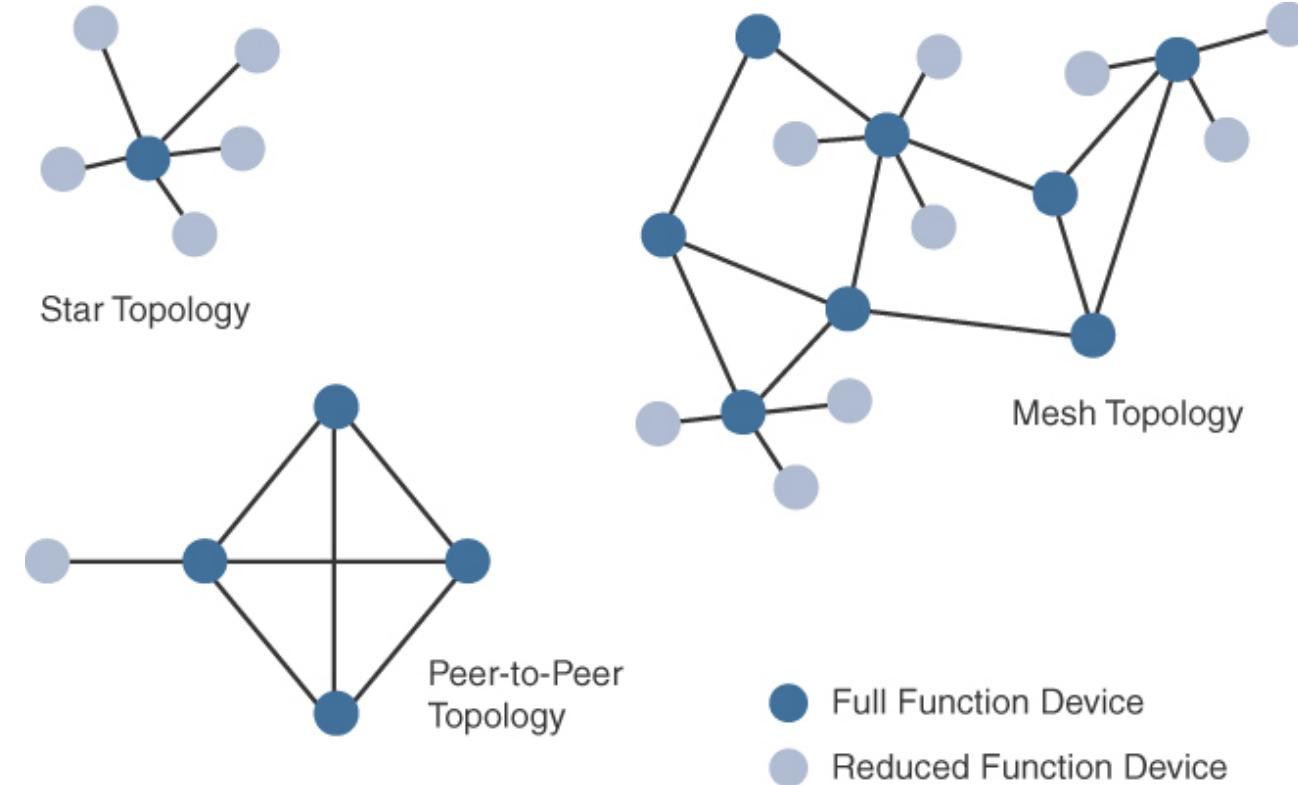
Mreža ograničenih resursa (1/2)

Constraint network, low-power and lossy networks (LLNs)

- bežična mreža čvorova s ograničenim izvorom energije
- potencijalno dugi periodi neaktivnosti čvorova (čak do 99% vremena), mali generirani promet
- ograničena širina pojasa i propusnost: od nekoliko do par stotina kbit/s
- „težak“ radijski kanal
 - nelicencirani spektar (*industrial, scientific, and medical, ISM*)
 - šum, interferencija, kolizija paketa
 - nestabilan sloj linka: česte i isprekidane pogreške ili potpuni gubitak veze
 - s obzirom na ograničenu propusnost, ne preporučuje se brza retransmisija: „*A constrained network that overreacts can lead to a network collapse—which makes the existing problem worse*“.

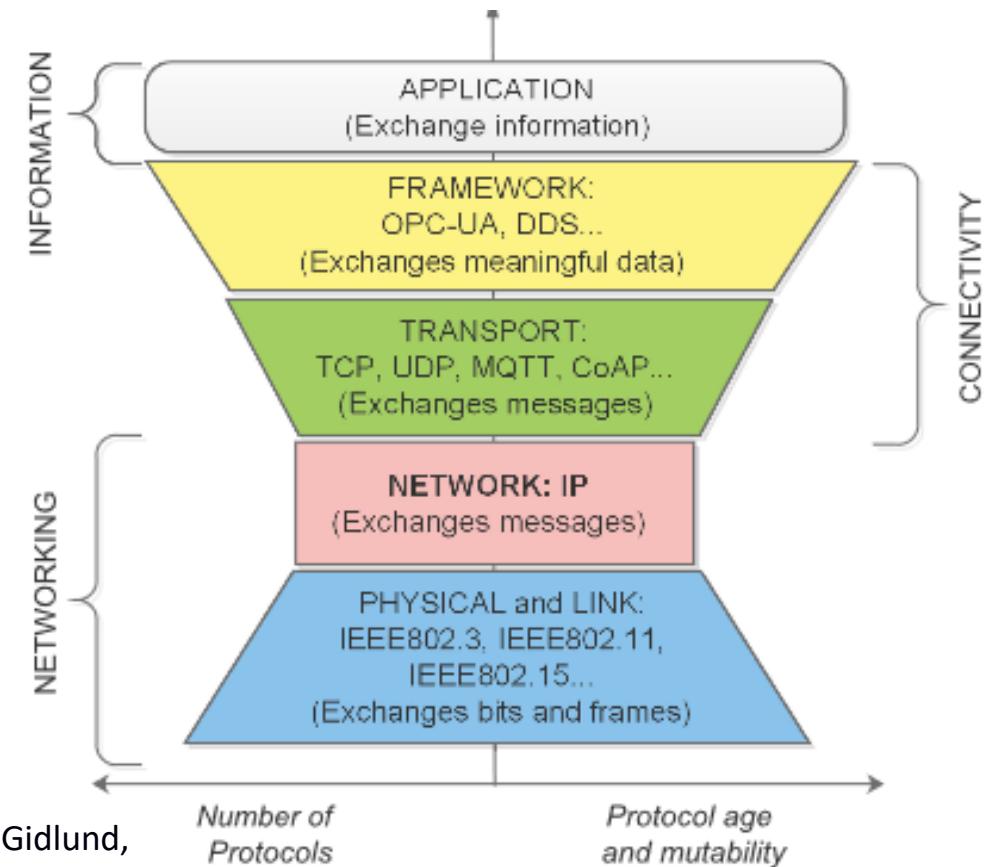
Mreža ograničenih resursa (2/2)

- Koriste sljedeće topologije: *star, mesh, P2P*
- Minimizirati signalizacijski promet
- Uzeti u obzir potrošnju energije za komunikaciju
- tipične pristupne tehnologije:
 - IEEE 802.15.4 (Wireless Personal Area Networks, WPAN),
 - IEEE 802.15.1 (Bluetooth),
 - LoRa i Sigfox (Low-Power Wide-Area, LPWA),
 - IEEE 802.11ah (Wi-Fi)



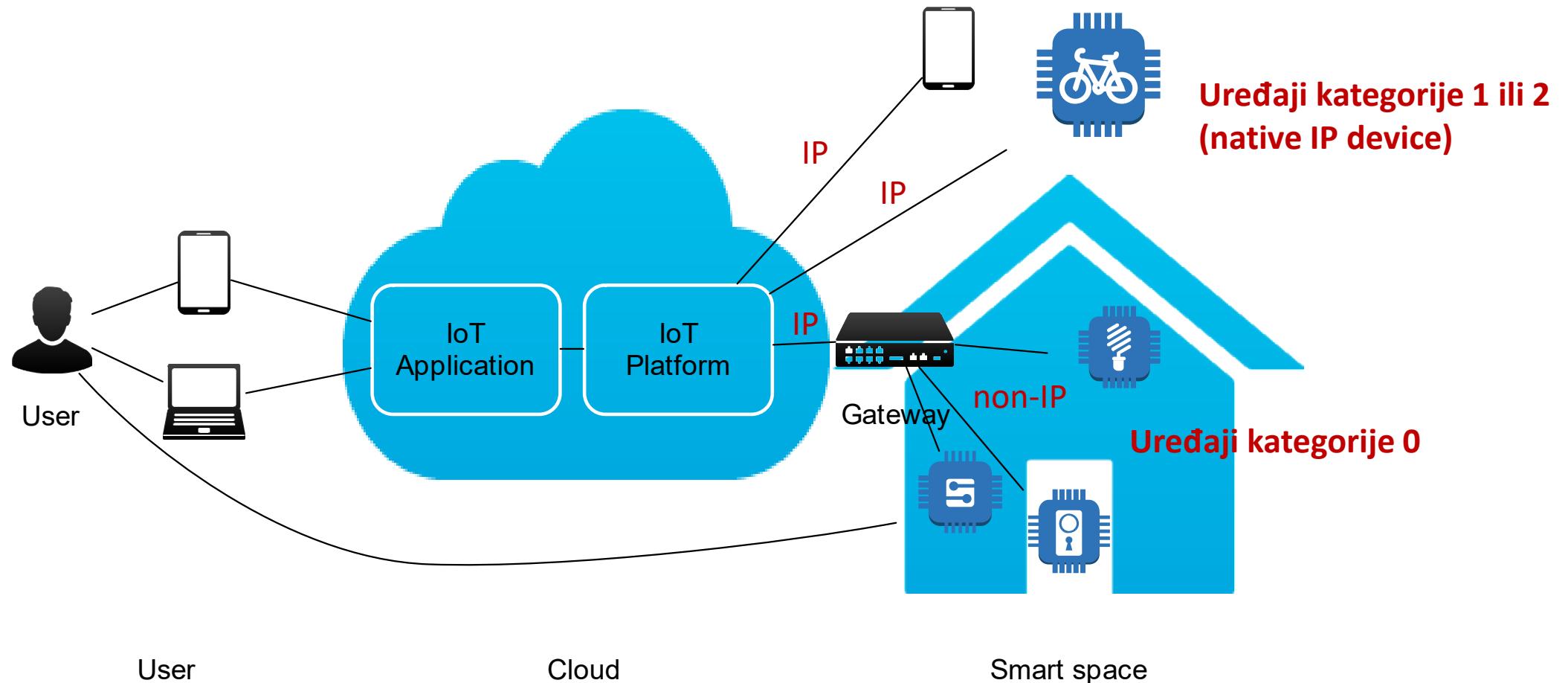
Zašto je IP prikladan za umrežavanje „stvari”?

- IP je jedinstven sloj neovisan o nižim i višim slojevima IP stack-a
- Otvoren, skalabilan, stabilan: IPv4 RFC 79 iz 1981, IPv6 RFC 2460 iz 1998
- Potrebne su optimizacije na svim slojevima IP stack-a s obzirom na ograničene resurse IoT-uređaja i mreža
- **Ponovite osnove protokola IP,
Komunikacijske mreže, 5. predavanje**



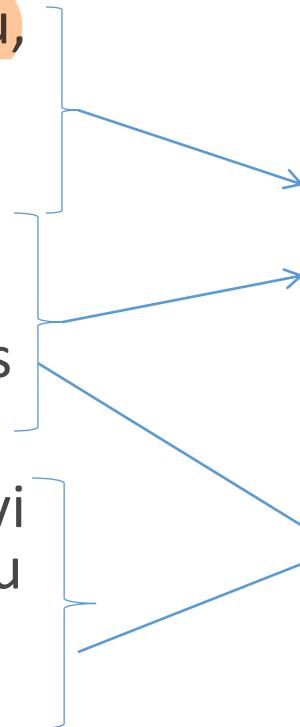
Izvor: E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund,
"Industrial Internet of Things: Challenges, Opportunities, and
Directions," in *IEEE Transactions on Industrial Informatics*, vol. 14, no.
11, pp. 4724-4734, Nov. 2018.

Prilagodba ili usvajanje IP-a



Kako umrežiti uređaje ograničenih resursa?

- Uređaji kategorije 0: rijetko komuniciraju, prenose nekoliko byte-ova, ograničene sigurnosne i upravljačke mehanizme
- Uređaji kategorije 1: imaju dovoljno resursa za implementaciju IP stack prilagođen hw za direktnu komunikaciju s poslužiteljem ili putem posrednika.
- Uređaji kategorije 2: resursi su usporedivi s resursima osobnog računala, podržavaju puni IP stack, ali treba voditi računa o ograničenjima pristupne tehnologije



Prilagodba (adaptation): koristi neku vrstu prilaza (gateway) za prijevod IP paketa na ne-IP pakete.

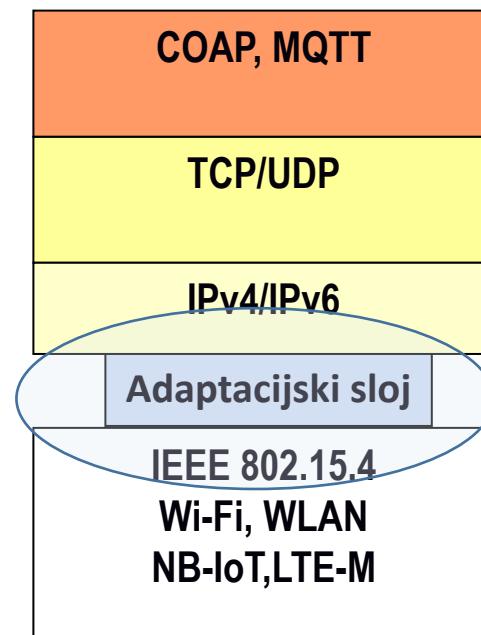
Usvajanje (adoption): zamjenjuje postojeće non-IP-slojeve IP-slojevima na samome uređaju.

Prilagodba protokolnog složaja za IoT

TCP/IP



IoT



Kako zapakirati IP pakete u okvire na nižem sloju podatkovne poveznice?

Treba li rješenje jednosmjernu ili dvosmjernu komunikaciju?

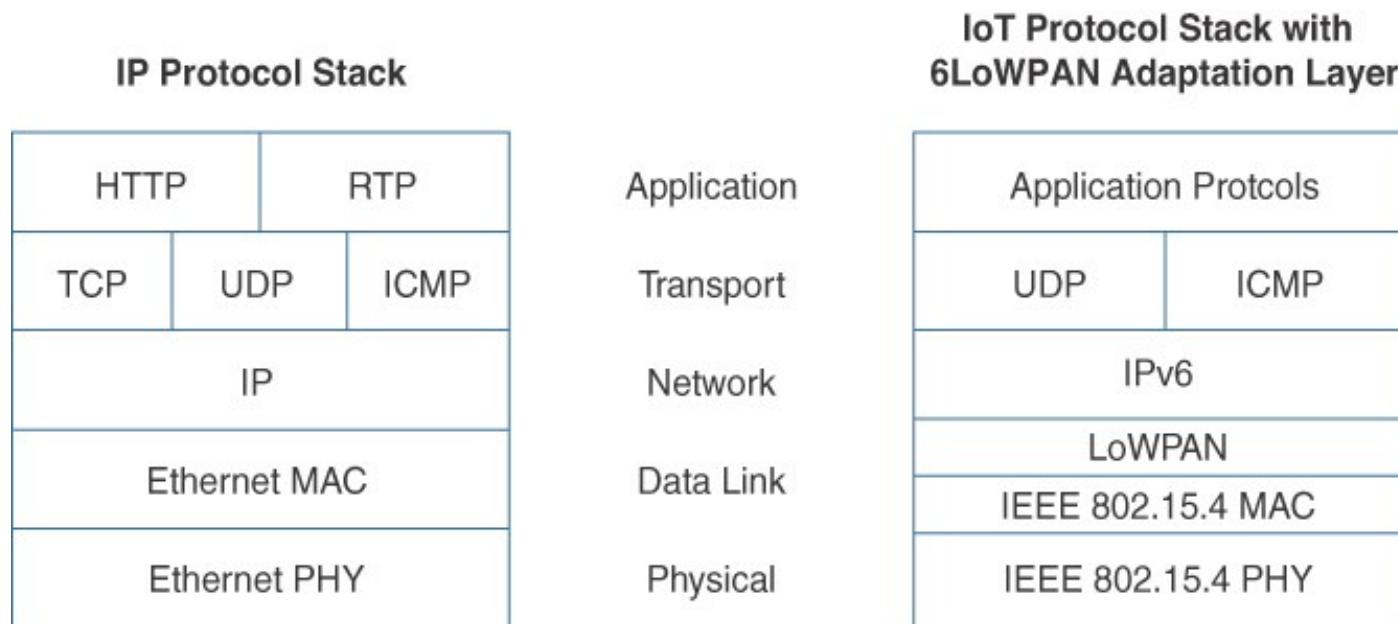
(Ako nije jednosmjerna, neće biti moguće udaljeno održavanje, software/firmware update)

Sadržaj

- Uređaji i mreže ograničenih resursa
- **6LoWPAN: IPv6 over Low Power Wireless Personal Area Networks**
- 6TiSCH: IPv6 over the TSCH mode of IEEE 802.15.4e
- RPL: IPv6 Routing Protocol for Low Power and Lossy Networks

Općenito o 6LoWPAN

- 6LoWPAN: IPv6 over Low Power Wireless Personal Area Networks
- prilagodba IP-a za **IEEE 802.15.4**



Cilj: optimizacija prijenosa IPv6-paketa u mrežama s ograničenim resursima (IEEE 802.15.4)

Izazovi za prilagodbu 6LoWPAN

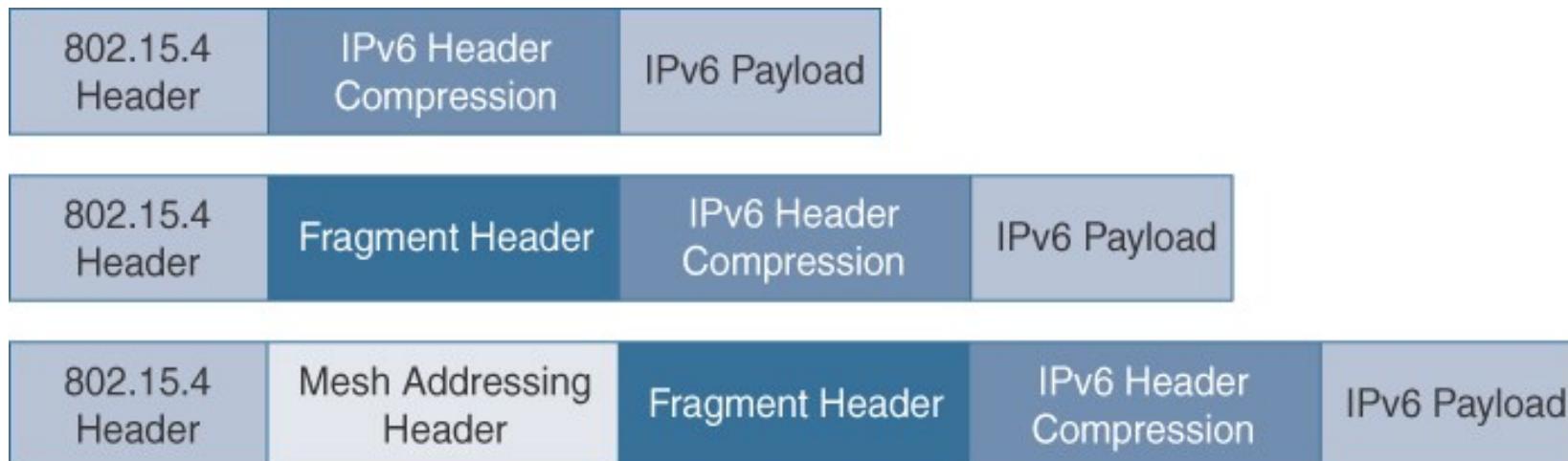
- Najmanji maximum transmission unit (MTU) za IPv6 je 1280 okteta, dok je 127 okteta najveća veličina okvira za IEEE 802.15.4
- Potrebni su **mehanizmi prilagodbe**:
 - Kompresija zaglavlja
 - Fragmentacija paketa
 - *Mesh*-adresiranje

Header Size Calculation

- IPv6 header is 40 octets, UDP header is 8 octets
- 802.15.4 MAC header can be up to 25 octets (null security) or $25+21=46$ octets (AES-CCM-128)
- With the 802.15.4 frame size of 127 octets, we have only following space left for application data!
 - $127-25-40-8 = 54$ octets (null security)
 - $127-46-40-8 = 33$ octets (AES-CCM-128)

Mehanizmi prilagodbe 6LoWPAN-a za IEEE802.15.4

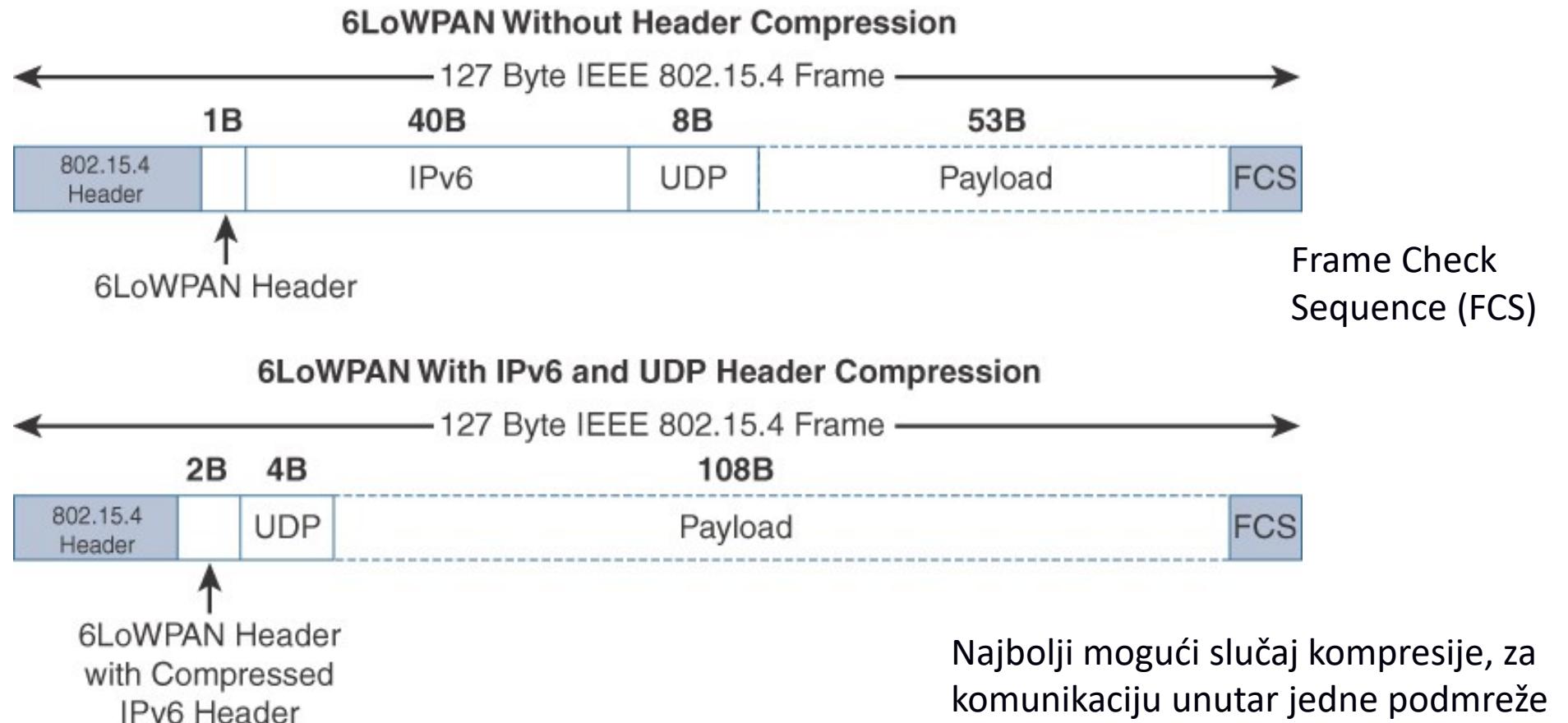
- RFC 4994: definira zaglavla za kompresiju, fragmentaciju i *mesh*-adresiranje
- U konkretnoj implementaciji se može koristiti kombinacija navedenih mehanizama



Kompresija zaglavlja

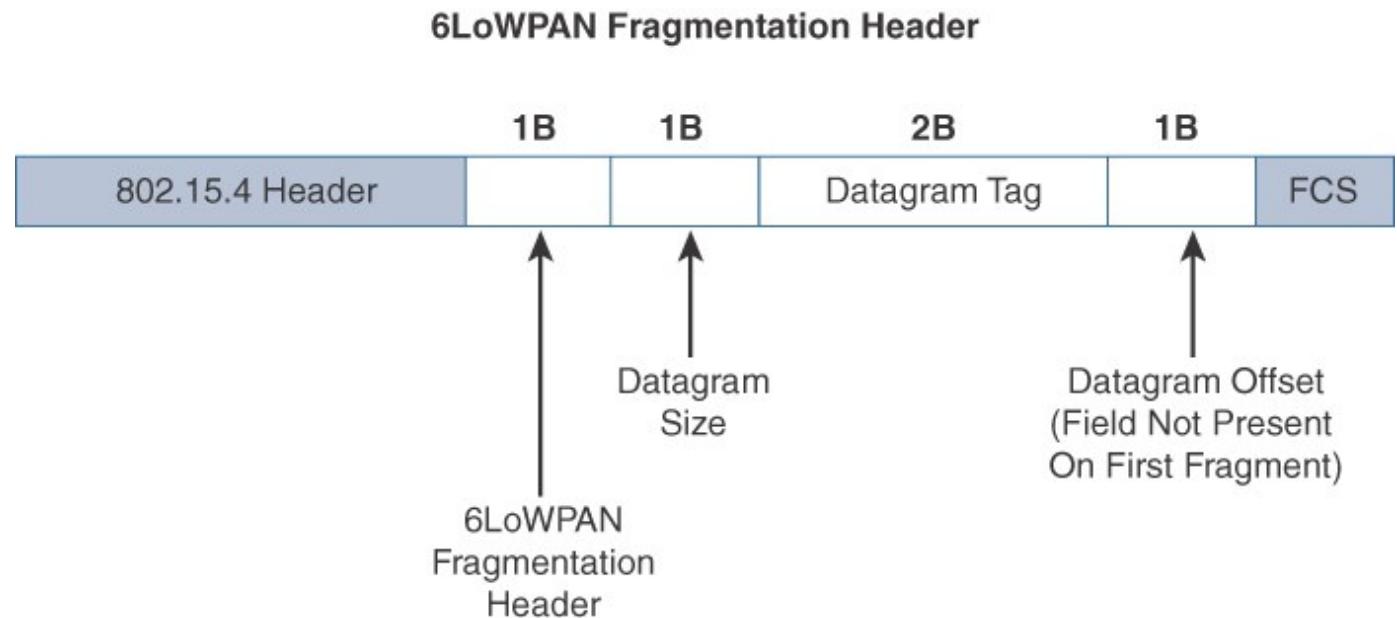
- Uklanja se redundantna informacija na nivou linka, mreže i transportnog sloja
 - Kompresija HC1 (IPv6 header) i HC2 (UDP header): može u nekim slučajevima kombinirano dva zaglavlja IPv6 (40-byte) i UDP (8-byte) svesti na 6 byte-a
 - Polja u zaglavljtu IPv6 se odbacuju kada ih sloj prilagodbe može zaključiti iz okvira 802.15.4
 - Koristi se jednostavna pretpostavka o dijeljenom kontekstu (lokalnoj podmreži)
 - Izostavljaju se standardna zaglavlja i pretpostavljaju opće korištene vrijednosti
- *Stateless*
- Definirana u RFC 4944 i RFC 6282

Kompresija zaglavlja (primjer)



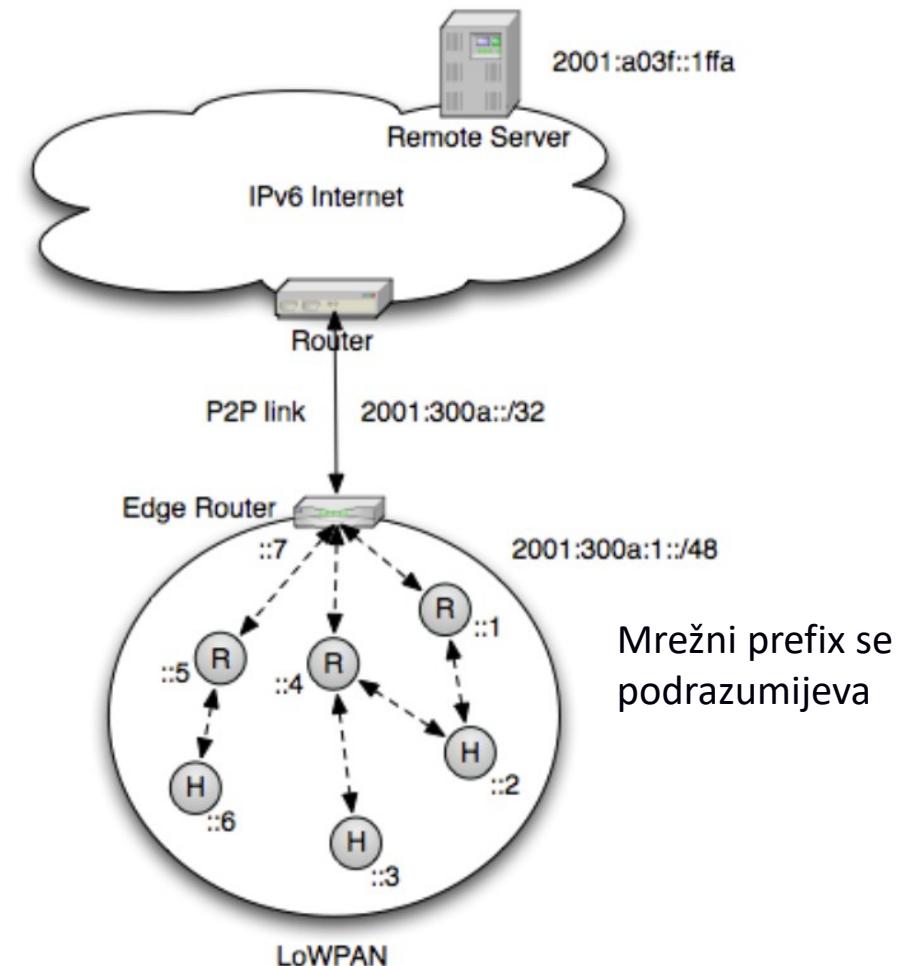
Fragmentacija

- Veliki paketi IPv6 (1280 bytes) se moraju razložiti na više manjih okvira 802.15.4 (127 bytes)
- Svi dijelovi (fragmenti) istog IP paketa imaju istu oznaku (*Datagram Tag*)
- *Datagram Size* definirana ukupnu veličinu originalnog paketa
- *Datagram offset* – pomak fragmenta u odnosu na paket
- Fragmenti ne moraju stići ispravnim redoslijedom, ali moraju unutar 60 s



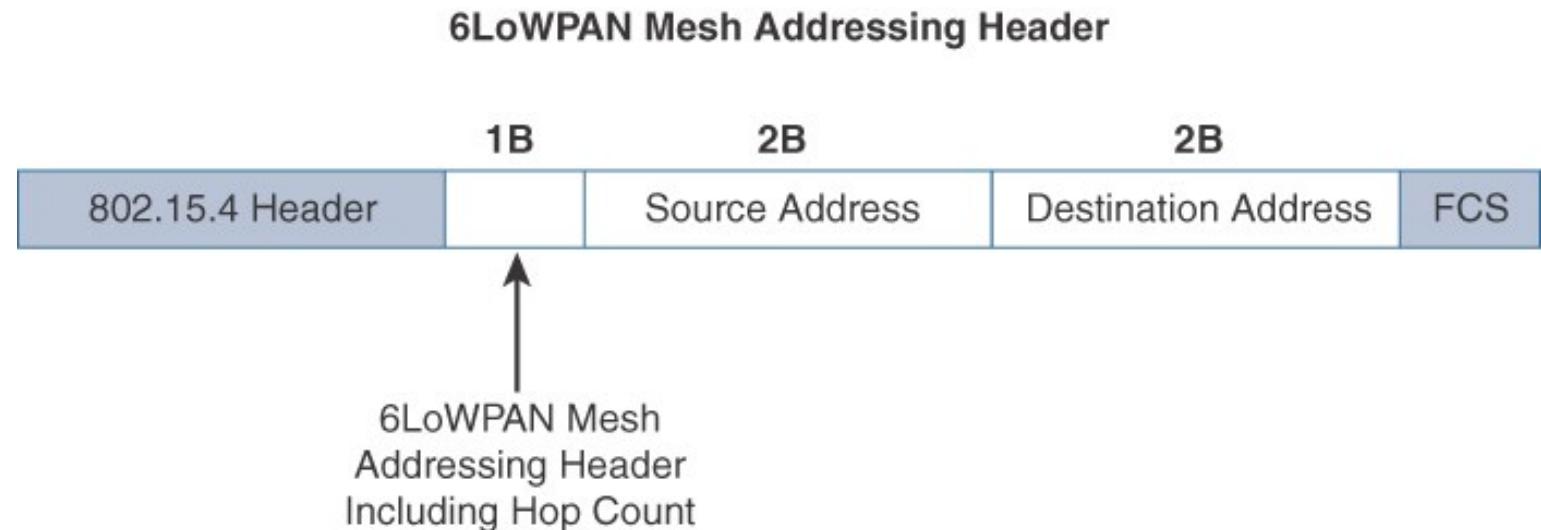
Mesh-adresiranje (1/2)

- za usmjeravanje paketa preko više čvorova ali u jednoj podmreži (naravno IEEE 802.15.4)
- prepostavka
 - *flat address spaces* (6LoWPAN mreža se razmatra kao 1 podmreža IPv6 s jedinstvenom MAC adresom)
- Kompresija IPv6 adresa za 6LoWPAN
 - izbacuju se svi podaci koji se mogu zaključiti iz „konteksta“
 - izbacuje se IPv6 prefix jer je poznat svim čvorovima u podmreži



Mesh-adresiranje (2/2)

- Zaglavje sadrži: Hop Limit, Source Address i Destination Address.
- Hop Limit: definira koliko puta se okvir može proslijediti, svaki čvor ga smanjuje za 1. Kada je 0, okvir se odbacuje
- Source Address i Destination Address:
IEEE 802.15.4 adrese

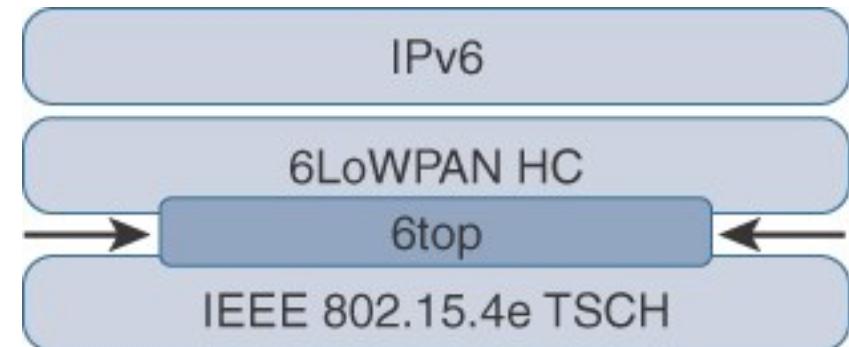


Sadržaj

- Uređaji i mreže ograničenih resursa
- 6LoWPAN: IPv6 over Low Power Wireless Personal Area Networks
- **6TiSCH: IPv6 over the TSCH mode of IEEE 802.15.4e**
- RPL: IPv6 Routing Protocol for Low Power and Lossy Networks

6TiSCH

- 6TiSCH: IPv6 over the TSCH mode of IEEE 802.15.4e
- IEEE 802.15.4e koristi Time-Slotted Channel Hopping (TSCH) koji se temelji na
 - **Time Division Multiple Access (TDMA)**: susjedni uređaji komuniciraju prema dogovorenom rasporedu koristeći alocirani vremenski odsječak (*time slot*)
- Pouzdanost komunikacije, pogodno za industrijske primjene



6top, a sublayer that glues together the MAC layer and 6LoWPAN adaptation layer.

6top

- 6top omogućuje višim slojevima upravljanje nad IEEE 802.15.4e uređajima: konfiguracija i kontrola procedura za upravljanje TSCH
- Potrebno je sinkronizirati slanje i primanje okvira pomoću posebnog *scheduling* algoritma koji definira kako se koriste vremenski odsječci.
- Scheduling utječe na propusnost, kašnjenje i potrošnju energije.
- 6top omogućuje susjednim čvorovima pregovaranje o ćelijama koje će koristiti za komunikaciju
 - ćelija definira vremenski odsječak i frekvencijski kanal za komunikaciju

6TiSCH schedule management mechanisms

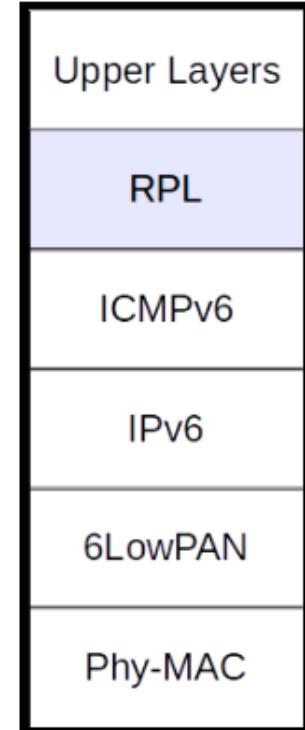
- **Statični:** svi čvorovi u mreži dijele statični raspored ćelija (raspored definira npr. administrator).
 - najjednostavniji mehanizam za implementaciju, predlaže se za inicijalnu komunikaciju
 - čvorovi su konstantno u stanju osluškivanja jer mogu primiti okvir u svakoj ćeliji, bespotrebno se troši puno energije.
- **Neighbor-to-neighbor scheduling:** definira se raspored na temelju opažanja komunikacije između čvorova.
 - Ćelije se dodaju ili oduzimaju u skladu s komunikacijskim potrebama.
- Detalji su definirani u **RFC 9030 An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)** iz svibnja 2021.

Sadržaj

- Uređaji i mreže ograničenih resursa
- 6LoWPAN: IPv6 over Low Power Wireless Personal Area Networks
- 6TiSCH: IPv6 over the TSCH mode of IEEE 802.15.4e
- **RPL: IPv6 Routing Protocol for Low Power and Lossy Networks**

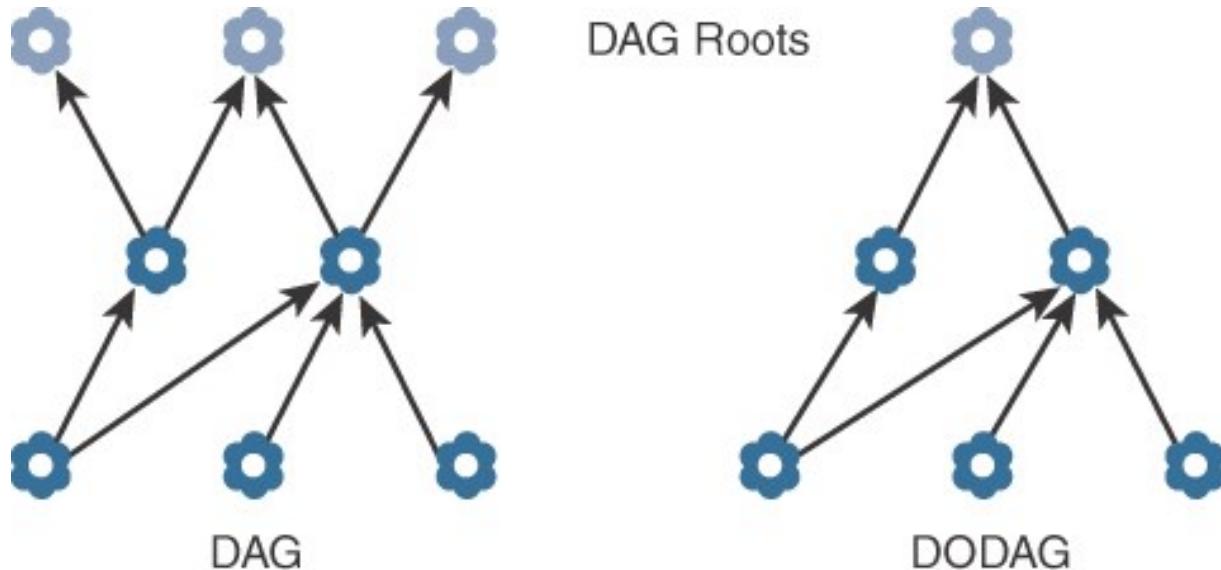
RPL

- IPv6 Routing Protocol for Low Power and Lossy Networks
- Definiran u RFC-u 6550
- Novi protokol za usmjeravanje paketa u mrežama ograničenih resursa (*distance-vector routing protocol*) na mrežnom sloju
- Svaki čvor može postati usmjeritelj (*mesh topologija*) na mrežnom sloju (*layer 3*) – postoje 3 vrste čvorova
- Izgrađuje se posebno stablo (DODAG) koristeći kontrolne poruke koje prenosi protokol Internet Control Message Protocol (ICMPv6) (stoga je RPL iznad sloja ICMPv6)
- Ne koristi informaciju s MAC sloja za usmjeravanje poruka



RPL: pretpostavke

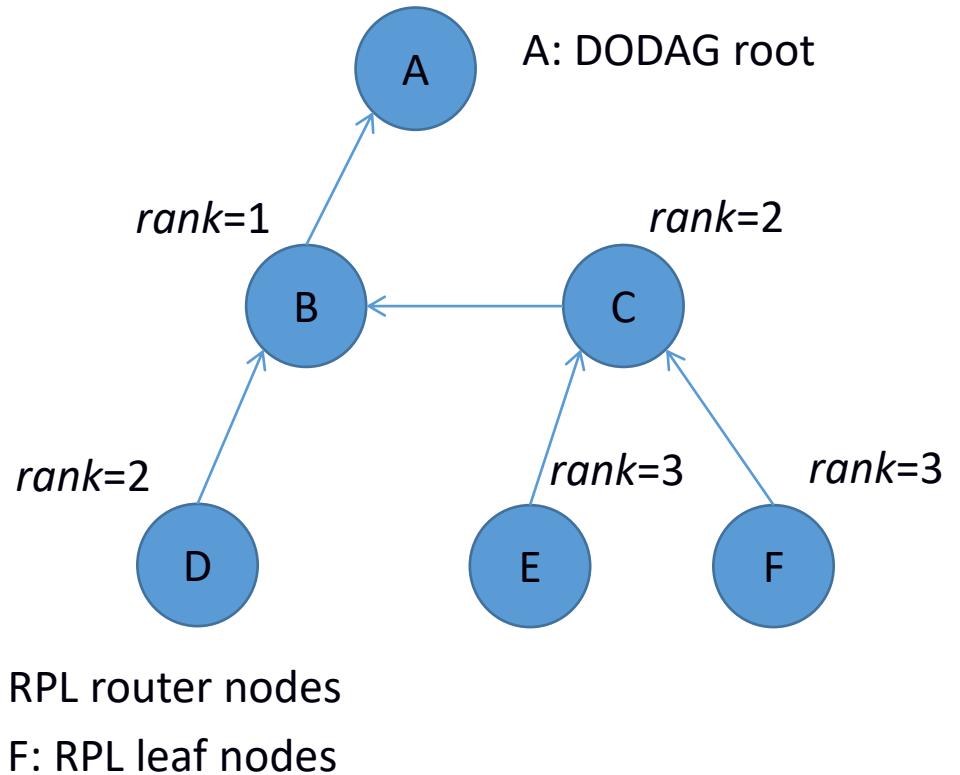
- **DAG: Directed Acyclic Graph**
 - Usmjereni graf bez usmjerenih petlji, poruka se u DAG-u ne može vratiti do čvora koji je izvorno generira
- **DODAG: Destination-Oriented DAG**
 - DAG s jednim korijenskim čvorom
 - svaki čvor održava do tri roditelja koji osiguravaju put do korijena (jedan je preferirani roditelj, tj. preferirani sljedeći skok za rute prema gore prema korijenskom čvoru)
 - Korijenski čvor za RPL zapravo je rubni usmjeritelj koji povezuje mrežu čvorova ograničenih resursa s Internetom



RPL DODAG: vrste čvorova

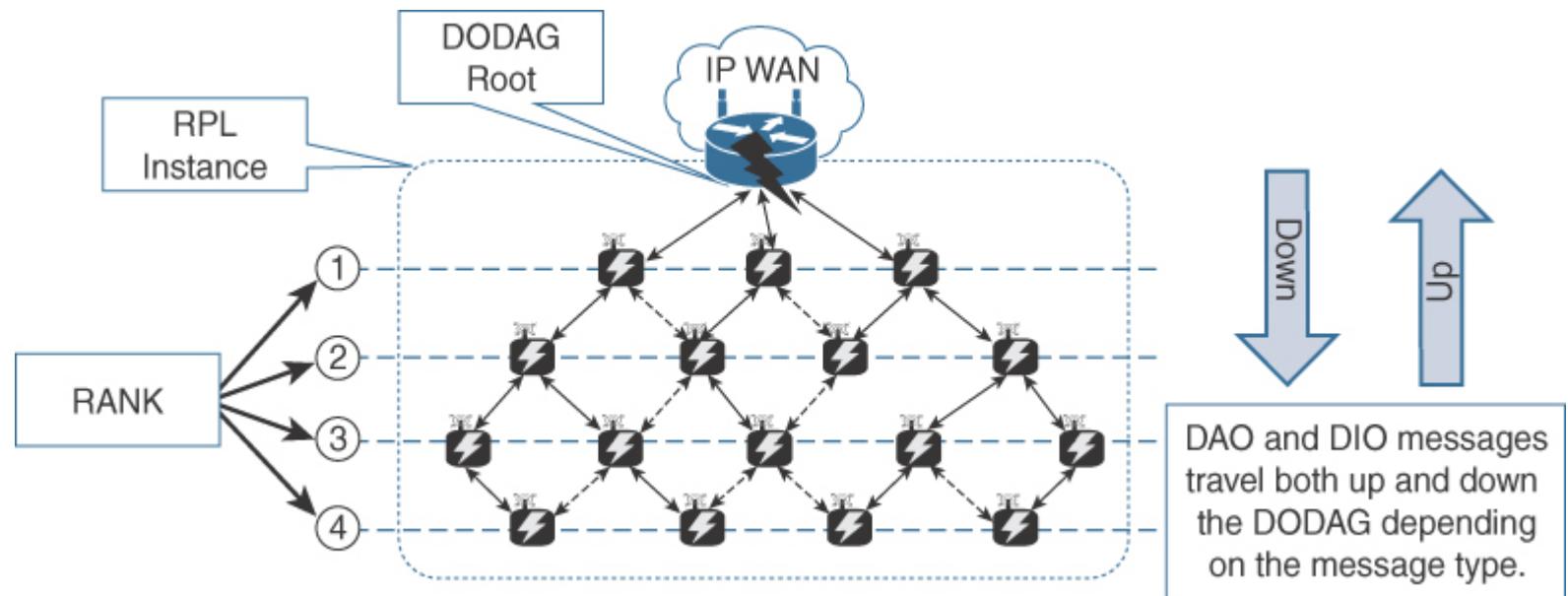
- **DODAG root:** korijenski čvor, zadužen za inicijalizaciju topologije, održava stanje (proaktivno) o topologiji DODAG. To je zapravo rubni usmjeritelj
- **RPL Router Node:** uređaj koji može generirati i usmjeravati RPL pakete. Nalazi se između čvorova root i leaf i sadrži routing info za sve svoje čvorove djecu (za storing mode).
- **RPL Leaf Node:** uređaj na dnu topologije i usmjerava samo vlastite pakete prema čvoru roditelju.

The rank is a rough approximation of how “close” a node is to the root and helps avoid routing loops and the count-to-infinity problem.



RPL: otkrivanje rute

- DODAG Information Solicitation (DIS)
- DAG Information Object (DIO)
- Destination Advertisement Object (DAO)



Kontrolne poruke RPL-a

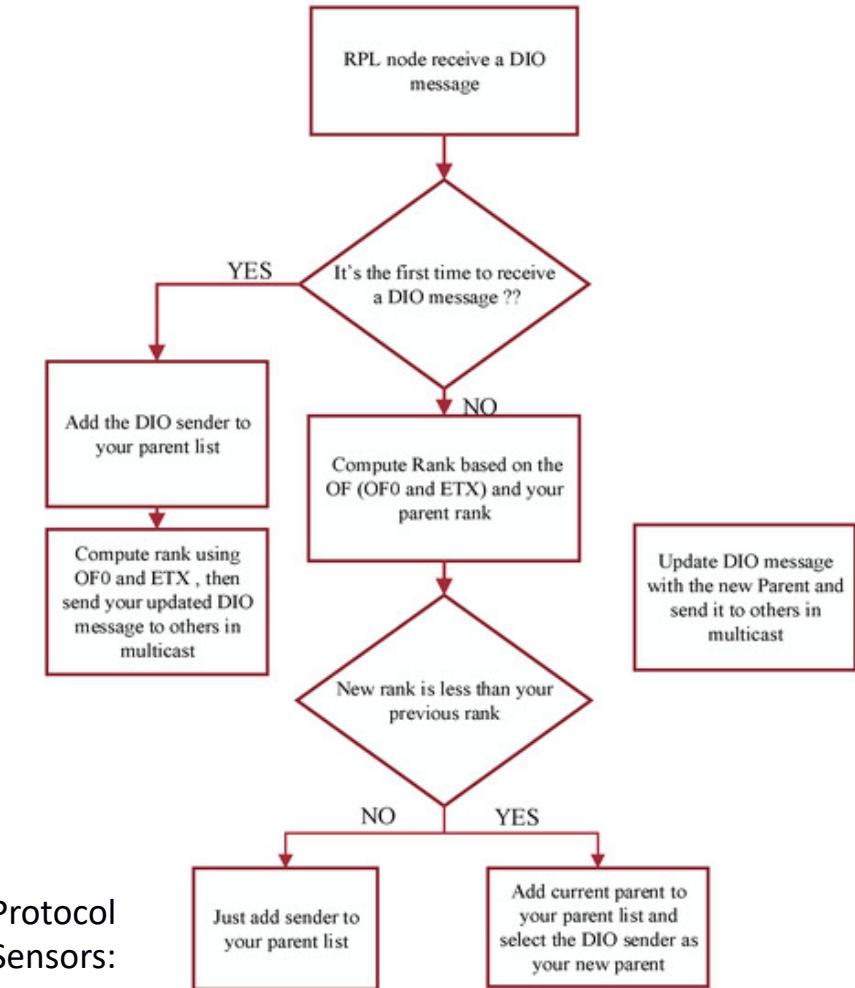
- **DODAG Information Solicitation (DIS)**: čvor šalje svojim susjedima kada od njih zahtijeva informaciju o usmjeravanju tj. DODAG Information Object (DIO). Poruka DIS je slična poruci Router Solicitation koju koristi protokol IPv6 Neighbour Discovery protocol
- **DODAG Information Object (DIO)**: odgovor na poruku DIS, sadrži informaciju o roditelju i rangu u DODAG-u, čvor je koristi kako bi održavao informaciju o DODAG-u u kojem se nalazi (tko mu je čvor-roditelj i koji mu je rang u DODAG-u), a može biti član i većeg broja DODAG-a
- **Destination Advertisement Object (DAO)**: omogućuje propagaciju informacije o svakom pojedinom čvoru prema korijenskom čvoru. Odgovor na DAO je poruka DAO-ACK.

RPL: dva načina rada

- **Storing mode:** Svi čvorovi održavaju potpunu tablicu usmjeravanja za jednu RPL domenu. Svaki čvor zna odrediti put prema svim ostalim čvorovima u podmreži RPL.
- **Non-storing mode:** Samo rubni usmjeritelj RPL domene sadrži potpunu tablicu usmjeravanja i zna odrediti put do krajnjeg čvora. Svi ostali čvorovi održavaju samo listu roditelja za usmjeravanje prema rubnom usmjeritelju.
 - Ovo je učinkovito rješenje na nivou čvora (štedi memoriju i CPU), ali koji su nedostaci?

Pravila za usmjeravanje poruka DIO

- služi za otkrivanje ruta prema korijenskom čvoru i odabir roditelja
- čvorovi kontinuirano primaju DIO poruke zbog promjena u topologiji mreže
- korijenski čvor pokreće izgradnju novog DODAG tako da šalje poruku DIO svojim susjedima, šalju se kao odgovor na poruku DIS
 - DODAGID: koristi se za identifikaciju korijenskog čvora i njegovog grafa DODAG



Izvor: Abdel Hakeem, S.A.; Hady, A.A.; Kim, H. RPL Routing Protocol Performance in Smart Grid Applications Based Wireless Sensors: Experimental and Simulated Analysis. *Electronics* **2019**, *8*, 186.

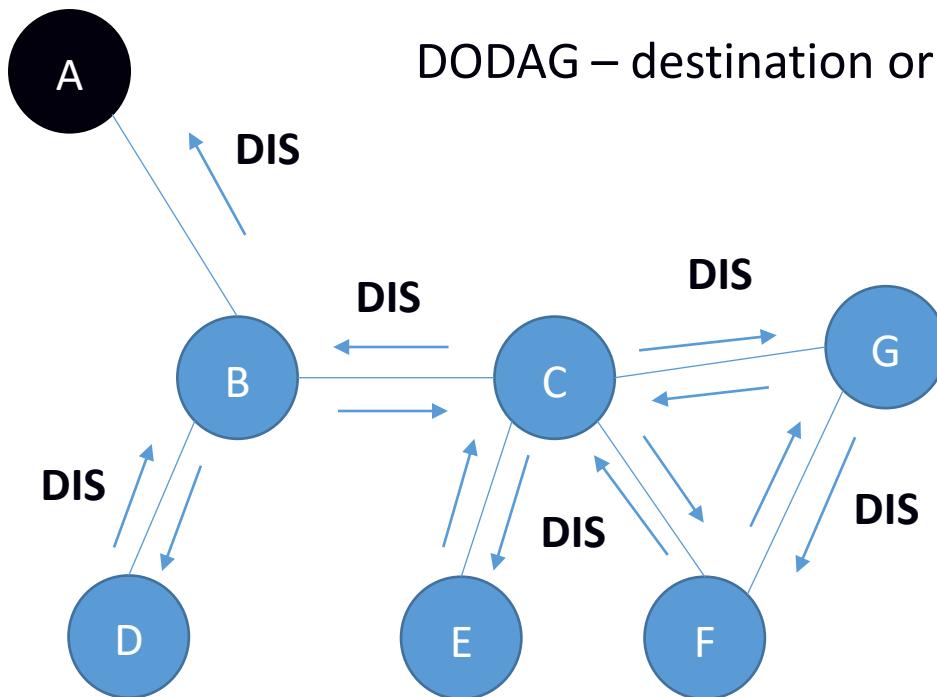
Pravila za usmjeravanje DAO

- DAO se koristi za kreiranje ruta od korijenskog čvora prema rubnim čvorovima
- čvorovi u DAO poruci **navode svoje roditelje** i šalju to poruku prema korijenskom čvoru
- DAO poruke su korisne i za roditeljske čvorove jer ih obavještavaju o „djeci” (*nodes are up and running*) te se koriste za održavanje tablice usmjeravanja na svim čvorovima (za **storing mode** rada)
- U slučaju **non-storing mode** DAO poruke se šalju samo do korijenskog čvora

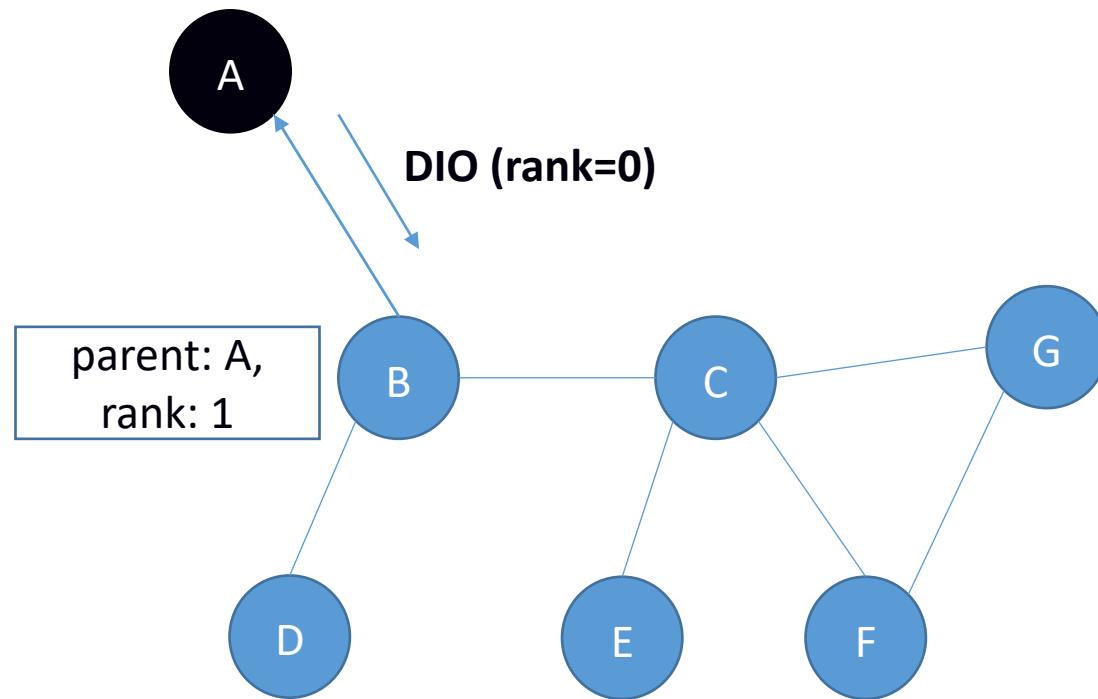
RPL – izgradnja grafa (1)

DIS - DODAG Information Solicitation

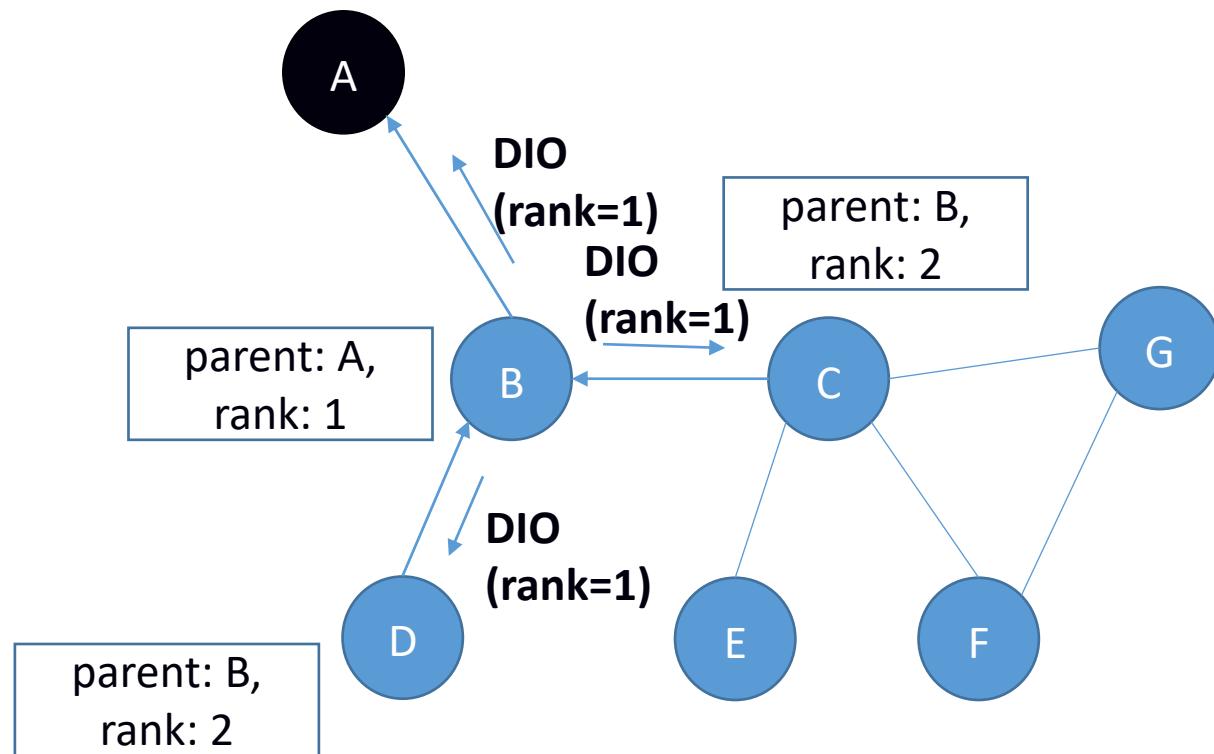
DODAG – destination oriented acyclic graph



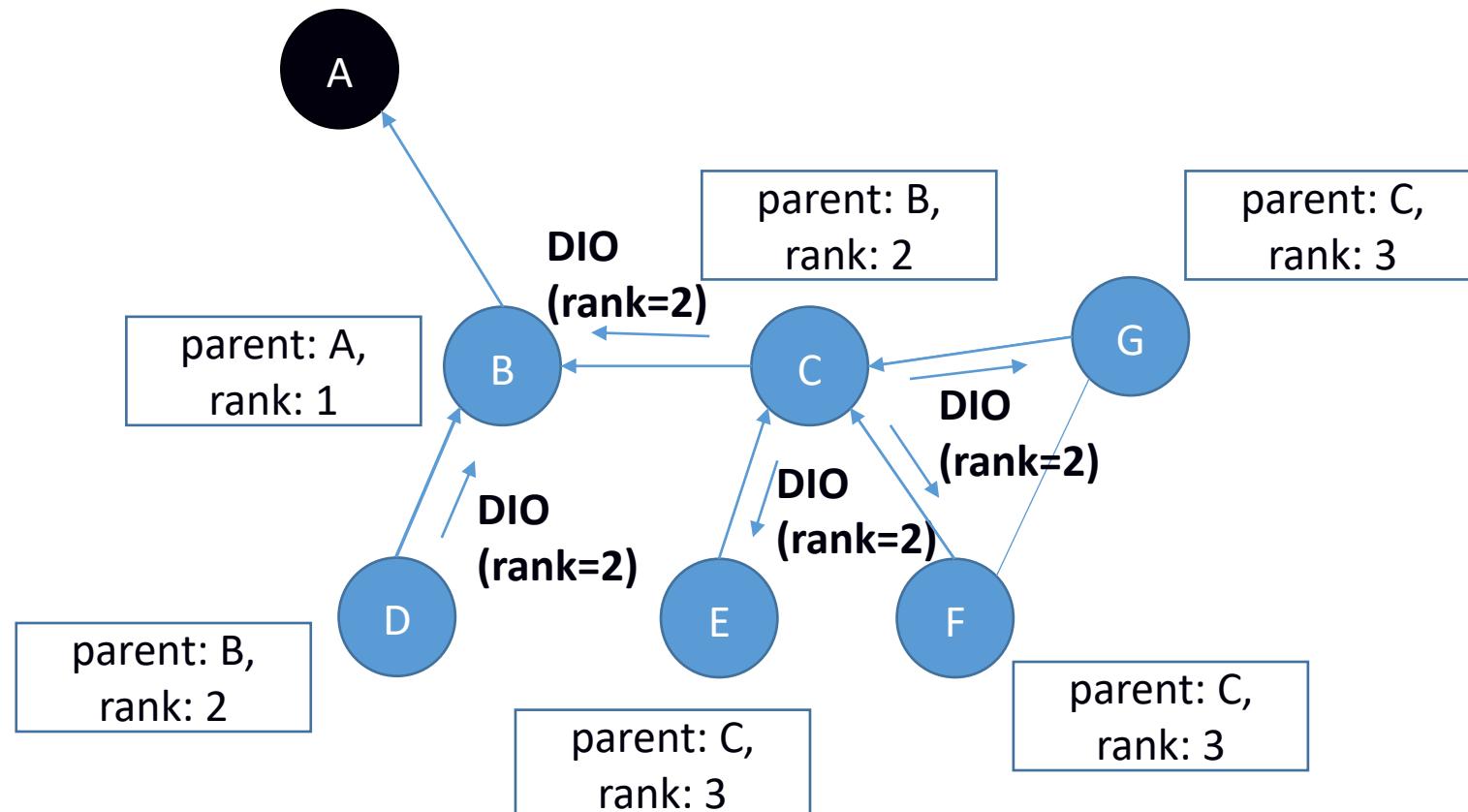
RPL – izgradnja grafa (2)



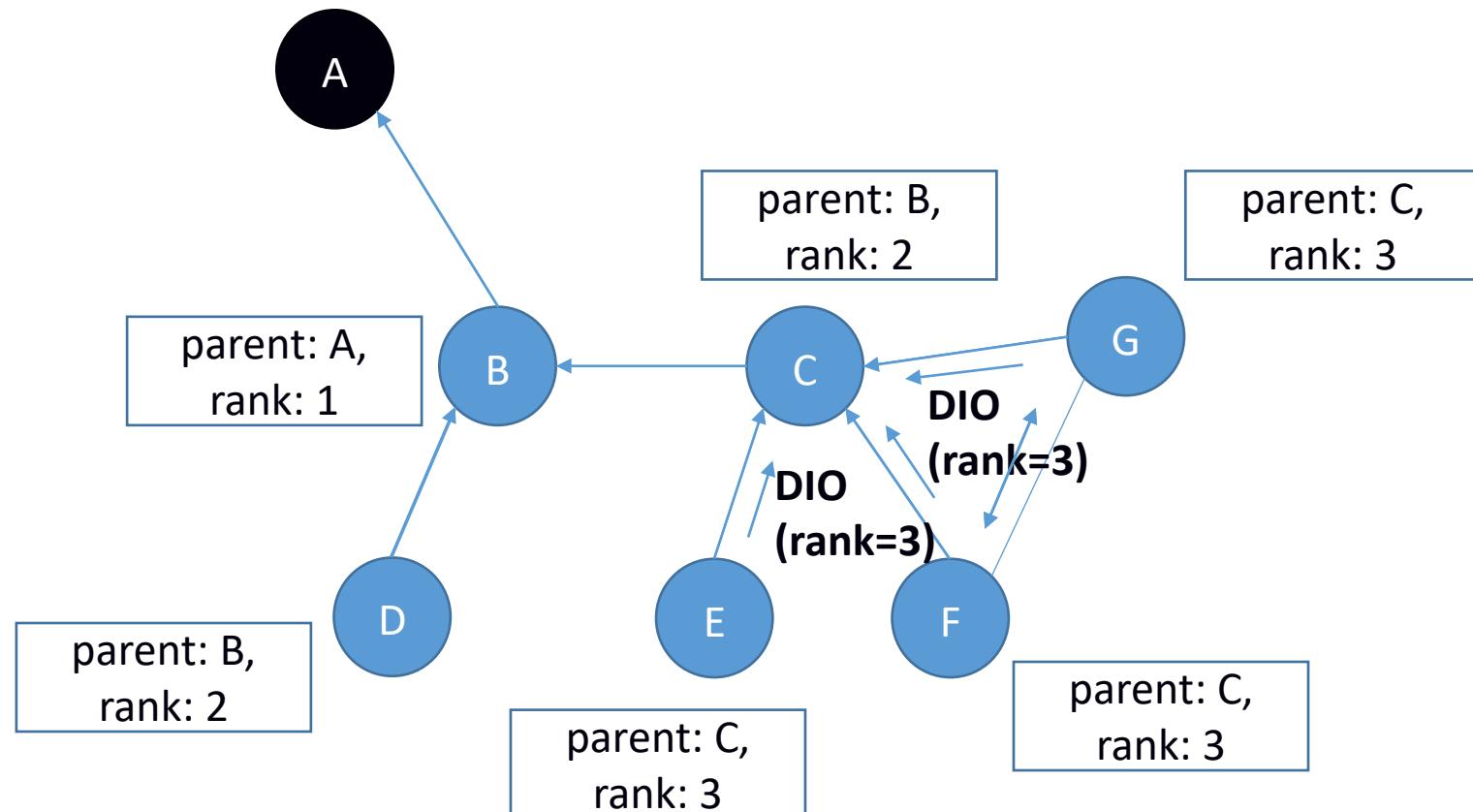
RPL – izgradnja grafa (3)



RPL – izgradnja grafa (4)



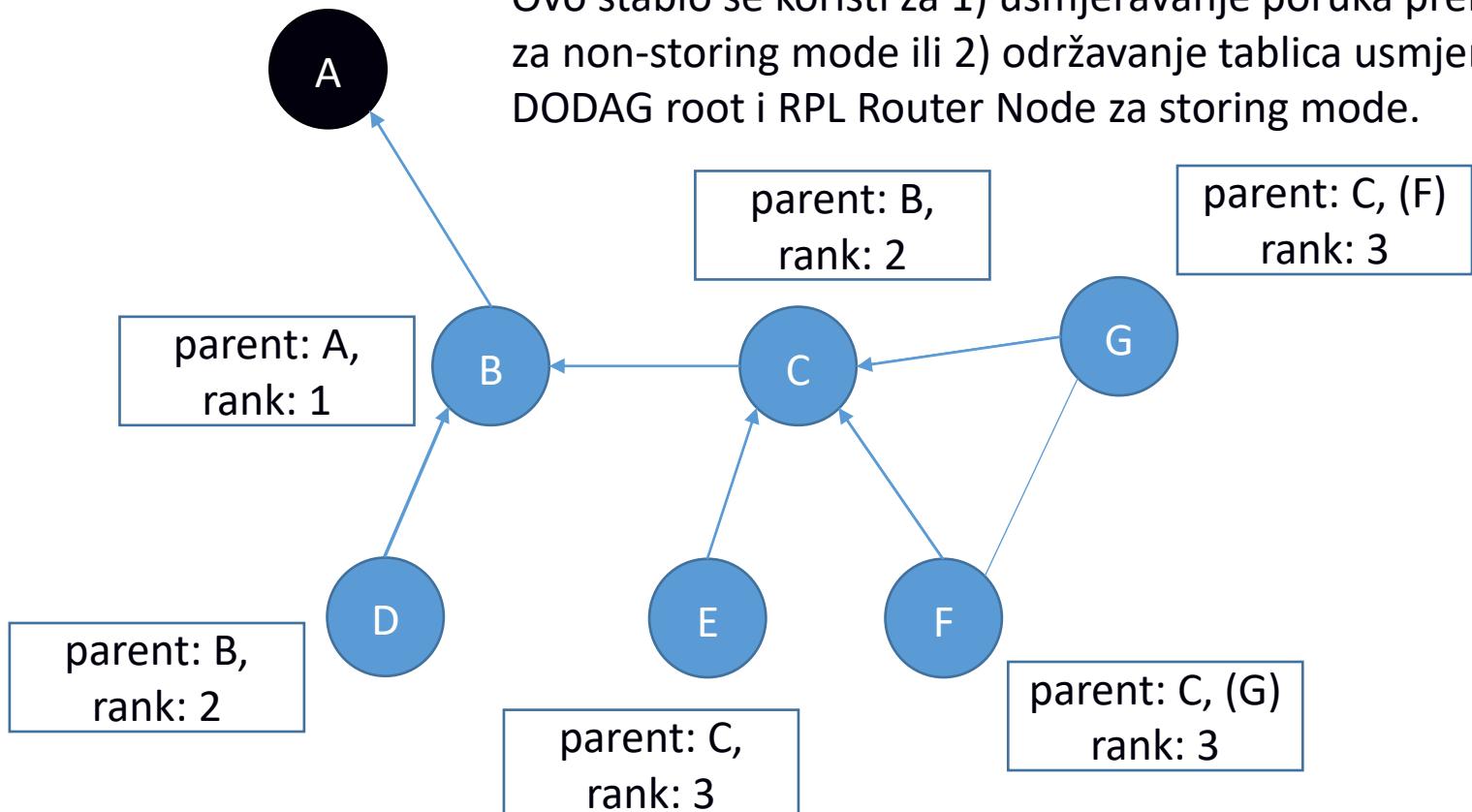
RPL – izgradnja grafa (5)



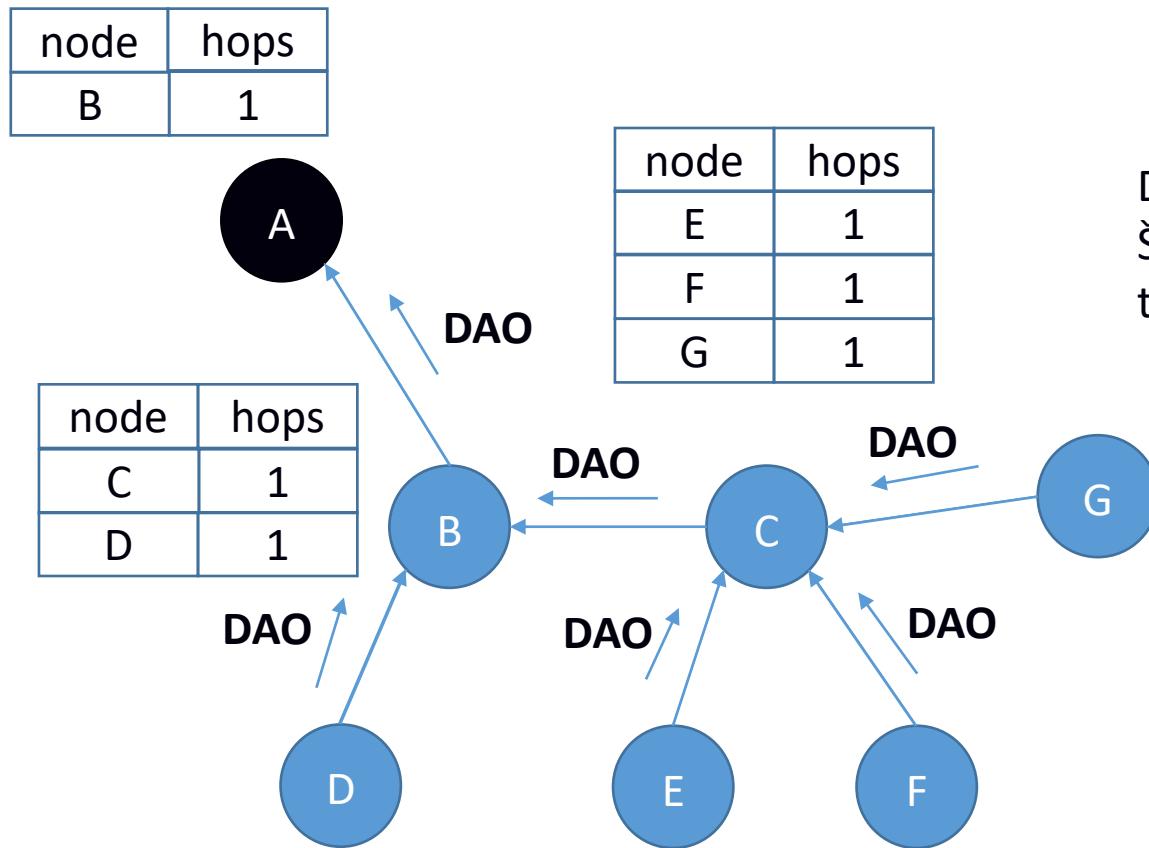
RPL – izgradnja grafa (6)

Nastalo je stablo (DODAG): svaki čvor ima primarnog roditelja (čvorovi F i G poznaju drugog potencijalnog roditelja).

Ovo stablo se koristi za 1) usmjeravanje poruka prema DODAG root za non-storing mode ili 2) održavanje tablica usmjeravanja na DODAG root i RPL Router Node za storing mode.



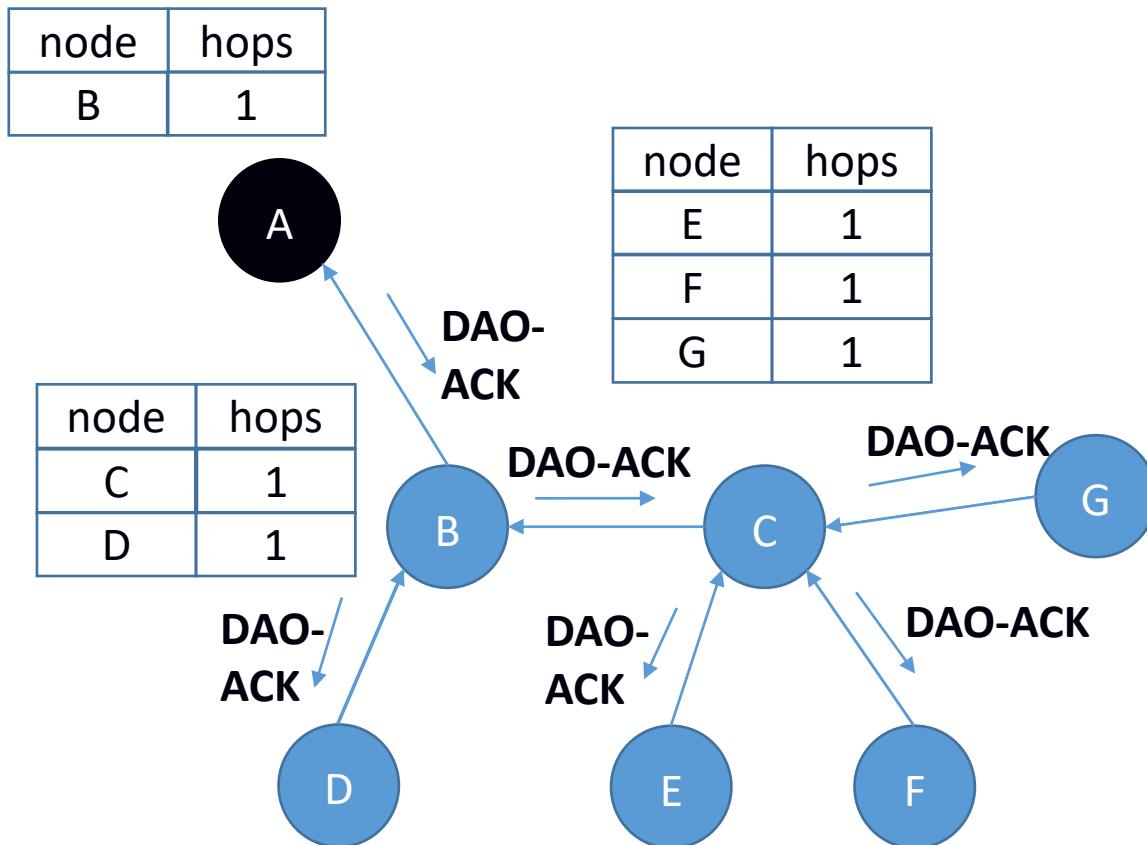
RPL – storing mode (1)



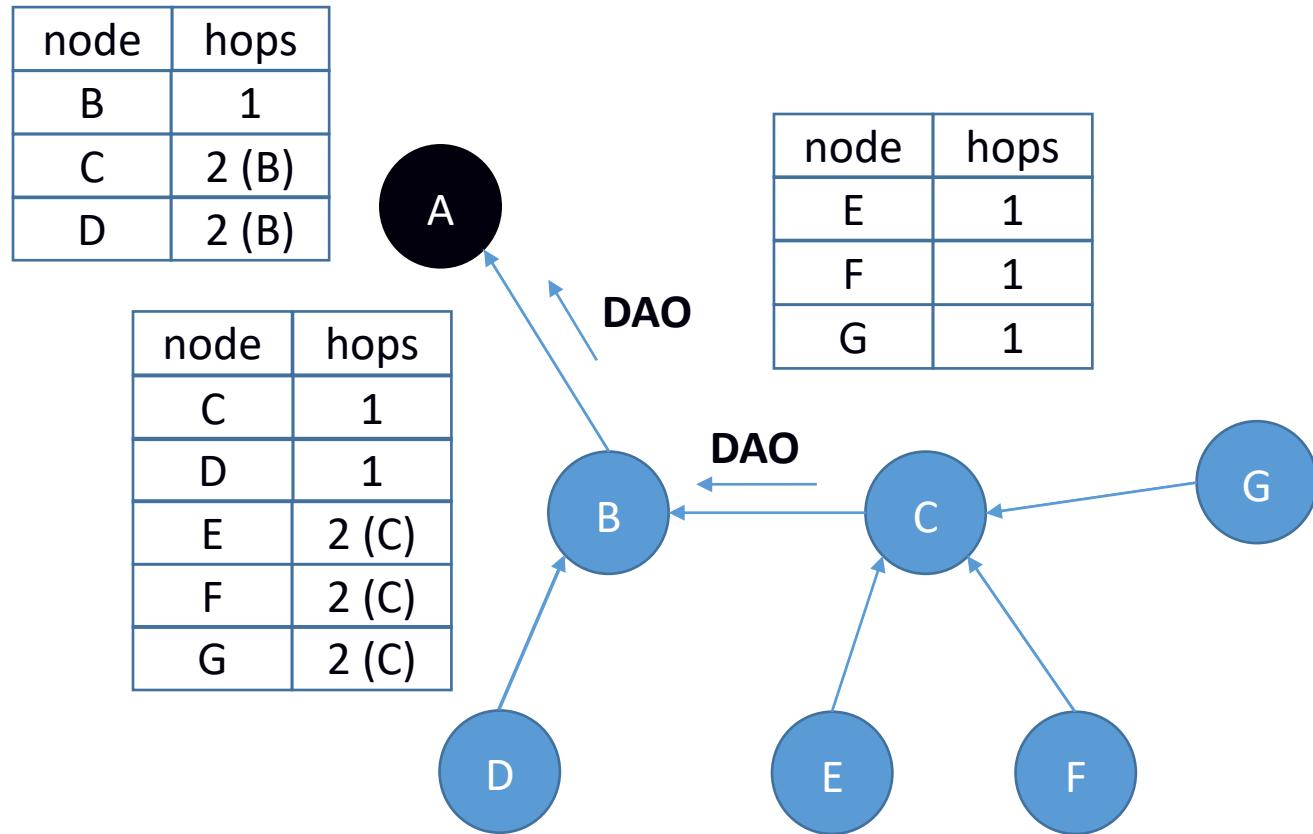
DAO - Destination Advertisement Object
Šalje čvor svome roditelju za održavanje
tablice usmjeravanja

non storing - manje memorije, bolja skalabilnost, duzi putevi, veca potrosnja energije

RPL – storing mode (2)



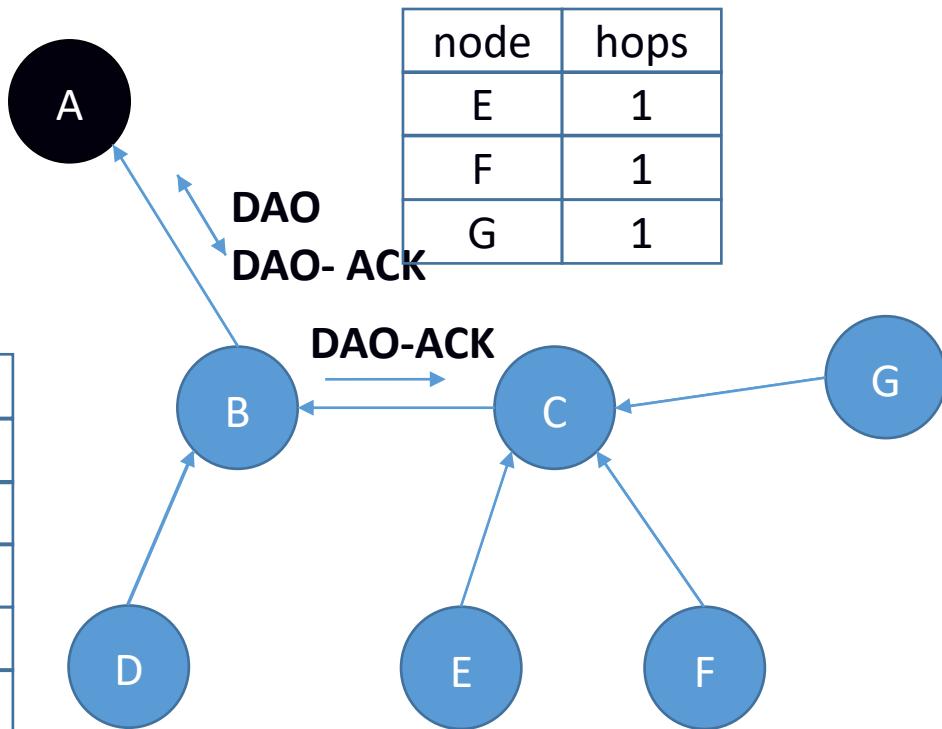
RPL – storing mode (3)



RPL – storing mode (4)

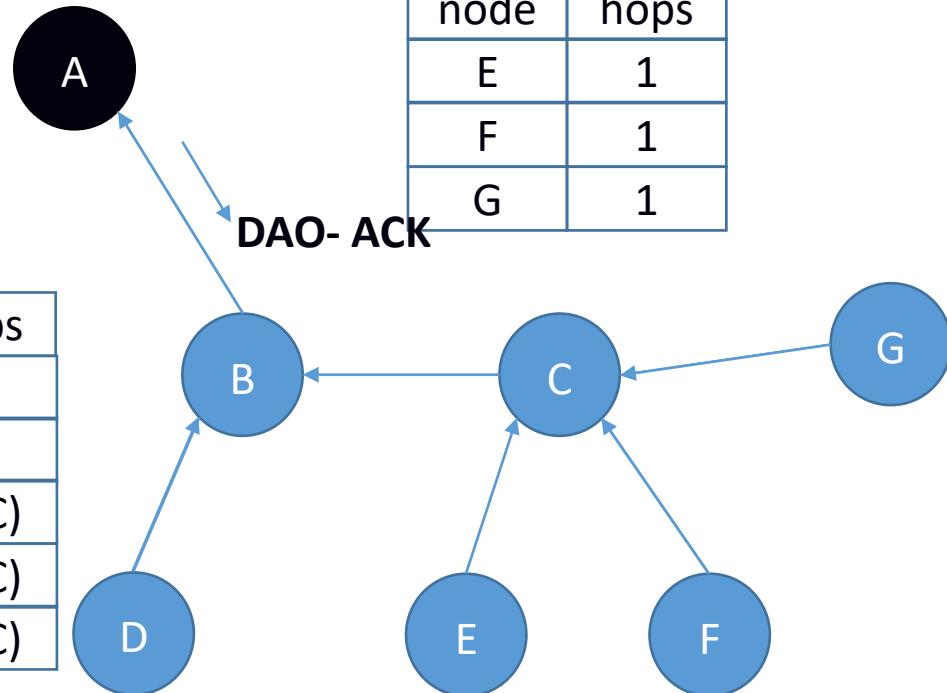
node	hops
B	1
C	2 (B)
D	2 (B)
E	3 (B)
F	3 (B)
G	3 (B)

node	hops
C	1
D	1
E	2 (C)
F	2 (C)
G	2 (C)

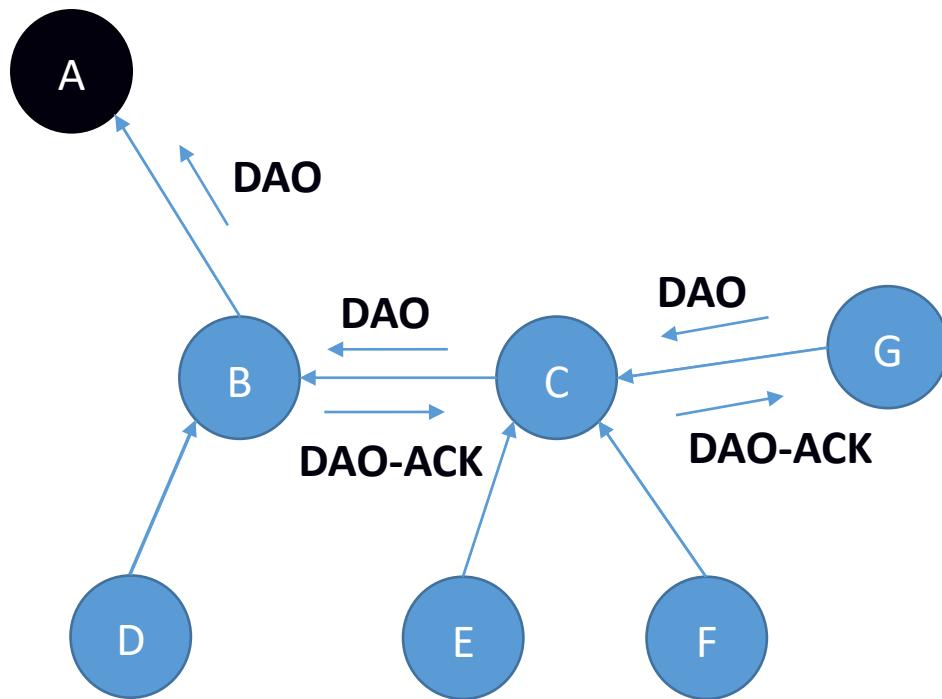


RPL – storing mode (5)

node	hops
B	1
C	2 (B)
D	2 (B)
E	3 (B)
F	3 (B)
G	3 (B)

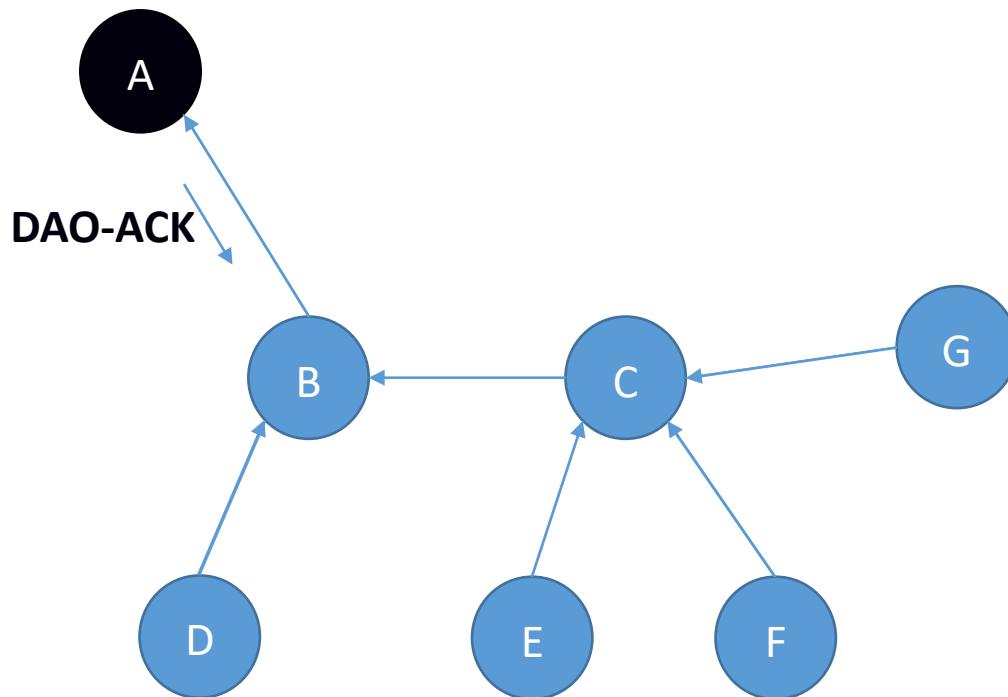


Non-storing mode (1)



Non-storing mode (2)

node	hops
B	1
C	2 (B)
D	2 (B)
E	3 (B-C)
F	3 (B-C)
G	3 (B-C)



Pitanja za ponavljanje

- Navedite obilježja različitih kategorija uređaja ograničenih resursa.
- Koja su obilježja mreže ograničenih resursa?
- Zašto je protokol IP pogodan za umrežavanje uređaja ograničenih resursa?
- Objasnite zašto je potrebna prilagodba protokola IPv6 za uređaje ograničenih resursa koji koriste IEEE 802.15.4. ObjASNITE mehanizme prilagodbe koje uvodi protokol 6LoWPAN.
- Objasnite što je DODAG i koje vrste čvorova koristi protokol RPL.
- Analizirajte prednosti i nedostatke non-storing modela rada protokola RPL.

Literatura

1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, and Jerome Henry. 2017. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things (1st ed.). Cisco Press. (5. poglavlje)
2. RFC 4944, Transmission of IPv6 Packets over IEEE 802.15.4 Networks, Sept. 2007 <https://tools.ietf.org/html/rfc4944>
3. RFC 6282, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, Sept. 2011 <https://tools.ietf.org/html/rfc6282>
4. RPL: <https://www.ietfjournal.org/roll-on-a-roll/>



SVEUČILIŠTE U ZAGREBU



Internet stvari

Diplomski studij

Računarstvo

Znanost o mrežama

Programsko inženjerstvo i informacijski
sistemi

Računalno inženjerstvo

Informacijska i komunikacijska tehnologija

Automatika i robotika

Informacijsko i komunikacijsko inženjerstvo

Elektrotehnika i informacijska tehnologija

Audiotehnologije i elektroakustika

Elektroenergetika

(Izborni predmet profila)

**7. Sigurnosni aspekti, upravljanje
uredjajima**

Ak. god. 2022./2023.

Zanimljivosti...

- MIRAI botnet – kraj 2016.
 - Zločudni kôd koji cilja uređaje IoT (tipično kamere)
 - telnet/web – lista *default* imena i lozinki → bruteforce → zaraza
 - “2016 Dyn cyberattack”
 - <https://github.com/jgamblin/Mirai-Source-Code>
- Medicinski uređaji - primjer St. Jude's
 - Pacemaker – sučelje za provjeru stanja
 - Moguće mijenjati otkucaje srca i isprazniti bateriju...
- Automobili
 - Jeep 2015 - pristup CAN-u kroz firmware update
 - Provaljivanje alarmnih sustava - Calamp i Viper SmartStart
 - Stealing a Tesla in seconds: <https://www.youtube.com/watch?v=aVIYuPzmJoY>

Još zanimljivosti...

- Smart Locks Used by Airbnb Get Bricked by Software Update
 - <https://gizmodo.com/smart-locks-used-by-airbnb-get-bricked-by-software-upda-1797839523>
- Sustavi SCADA (Supervisory Control and Data Acquisition) / ICS
 - Industrija 4.0, elektrane... - automatizacija –
 - Sve više uređaja IoT → Industrial IoT (IIoT)
 - Stuxnet – crv koji je napadao Siemens PLC-ove
 - iranska nuklearna postrojenja
 - December 2015 Ukraine power grid cyberattack
 - Energetski sektori – SAD, UK
 - Finska – sustavi grijanja

Problemi sigurnosti i privatnosti u IoT

- Uzroci loše sigurnosti u IoT (vrijede i općenito)
 - Fokus je na funkcionalnosti uređaja / sustava
 - Fokus je na sučeljima prema korisnicima
 - Pokušava se skratiti vrijeme razvoja kako bi proizvodi čim prije izašli na tržiste (konkurenčija)
- Što je s podacima korisnika?
 - Uređaji IoT ih prikupljaju
 - Prenose se u "oblak" i obrađuju
 - Curenje podataka?

Složaj tehnologija u IoT...

- Napadači “poznaju” tehnologije i imaju alate
 - Automatizirani alati za napad na pojedine slojeve / tehnologije
 - Poznate ranjivosti za većinu slojeva u složaju
- Razvijatelji nisu sigurnosni stručnjaci
 - Ne postoje gotova rješenja / alati
 - Ne postoje metodologije impl. sigurnosti
- Što se događa?
 - Razvijatelji razviju komponente i integriraju ih u sustav
 - Ostaje velika “površina napada” preko cijelog složaja
 - Iskusnim napadačima nije problem pronaći i iskoristiti ranjivost



OWASP



- Open Web Application Security Project
- Top 10
 - Web, mobilne aplikacije, IoT
- Smjernice za razvoj sigurnih aplikacija/usluga
 - i testiranje nesigurnih aplikacija/usluga
- Alati – npr. ZAP
- Application Security Verification Standard (OWASP ASVS)
 - “kuharica” za izradu sigurnih (web) aplikacija
 - Donekle primjenjivo i na ostale domene!

OWASP Top 10 IoT – 2014

- I1 Nesigurna sučelja weba (Insecure Web Interface)
- I2 Nedovoljna autentifikacija / autorizacija (Insufficient Authentication/Authorization)
- I3 Nesigurne mrežne usluge (Insecure Network Services)
- I4 Nedostatak šifriranja u transportu (Lack of Transport Encryption)
- I5 Privatnost (Privacy Concerns)
- I6 Nesigurna sučelja u oblaku (Insecure Cloud Interface)
- I7 Nesigurna mobilna sučelja (Insecure Mobile Interface)
- I8 Konfiguracija sigurnosnih postavki (Insufficient Security Configurability)
- I9 Nesigurni software/firmware (Insecure Software/Firmware)
- I10 Loša fizička sigurnost (Poor Physical Security)

OWASP Top 10 IoT – 2018

- I1 Loše lozinke - Weak Guessable, or Hardcoded Passwords
- I2 Nesigurne mrežne usluge - Insecure Network Services
- I3 Nesigurna sučelja - Insecure Ecosystem Interfaces
- I4 Nesigurni mehanizmi nadogradnji - Lack of Secure Update Mechanism
- I5 Zastarjele komponente - Use of Insecure or Outdated Components
- I6 Loša privatnost - Insufficient Privacy Protection
- I7 Nedovoljno šifriranje - Insecure Data Transfer and Storage
- I8 Nedostatak upravljanja - Lack of Device Management
- I9 Loše početne postavke - Insecure Default Settings
- I10 Fizička sigurnost - Lack of Physical Hardening

OWASP IoT Top 10 2014

I1 Insecure Web Interface

I2 Insufficient Authentication/Authorization

I3 Insecure Network Services

I4 Lack of Transport Encryption/Integrity Verification

I5 Privacy Concerns

I6 Insecure Cloud Interface

I7 Insecure Mobile Interface

I8 Insufficient Security Configurability

I9 Insecure Software/Firmware

I10 Poor Physical Security

OWASP IoT Top 10 2018 Mapping

I3 Insecure Ecosystem Interfaces

I1 Weak, Guessable, or Hardcoded Passwords

I3 Insecure Ecosystem Interfaces

I9 Insecure Default Settings

I2 Insecure Network Services

I7 Insecure Data Transfer and Storage

I6 Insufficient Privacy Protection

I3 Insecure Ecosystem Interfaces

I3 Insecure Ecosystem Interfaces

I9 Insecure Default Settings

I4 Lack of Secure Update Mechanism

I5 Use of Insecure or Outdated Components

I10 Lack of Physical Hardening



I1 Weak Guessable, or Hardcoded Passwords

- Korištenje jednostavnih lozinki
- Statičke lozinke ili tokeni (posebno kod “manjih” uređaja)
- Korištenje slabih i predvidljivih tokena / identifikatora sjednica?
- Osnovne provjere:
 - Mogu li postaviti jednostavnu lozinku (npr. qwerty)?
 - Istiće li sjednica nakon nekog vremena?
 - Mogu li promijeniti *default* ime i lozinku?
 - Hoće li me aplikacija “zaključati” nakon n pogrešnih lozinki?
 - Mogu li nekako doći do podataka korisnika (Zaboravljena lozinka?)
 - Penetracijsko testiranje sučelja “izvana”
 - a poželjno i kao registrirani korisnik

I2 Insecure Network Services

- Uz osnovne usluge nužne za funkcioniranje uređaja IoT često su pokrenuti različiti servisi
 - Jesu li svi servisi doista potrebni?
 - Ako jesu, je li verzija / implementacija sigurna (CVE liste)?
 - Jesu li adekvatno zaštićeni (npr. I3)?
- Osnovne provjere:
 - Skeniranje *portova* kako bi se utvrdilo što je sve pokrenuto (nmap)
 - Provjera ranjivosti otvorenih servisa (npr. Nessus, OpenVAS)
 - Fuzzing, buffer overflow → tipičan cilj: DoS
 - Posebno paziti na UPnP portove (Universal Plug&Play)

Alati za skeniranje i lista ranjivosti



Results (278 of 278)

Results by Severity Class (...):
High: 1, Medium: 62, Low: 159, Log: 56.

Results vulnerability word ...:
POODLE, Insufficient, Execution, Deprecated, DCE/IPC, Multiple, Microsoft, NTLM, MSRPC, Strength, Vulnerabilities, Using, Service, Report, LDAP, Algorithms, SMB, TCP, timestamps, Cipher, JS, Suites, request, MAC, SSL/TLS, Signed, CBC, Reporting, Weak, Enumeration, Check, Services, SSH enabled, Supported, Vulnerability, from, Information, retrieve, Certificate, Protocol, search, Group, Encryption, Windows, SMBv1, Signature, Server, SSLv3, SSLv2, Detection, Disclosure, Algorithm, Key.

Results by CVSS (Total: 278):

CVSS Score Range	Count
N/A	0
1	0
2	0
3	50
4	30
5	115
6	5
7	5
8	5
9	5
10	45

Vulnerability:

Vulnerability	Severity	QoD	Host	Location	Created
SMBv1 enabled (Remote Check)	10.0 (High)	80%	127.0.0.31	445/tcp	Thu Mar 23 16:33:27 2017
SMBv1 enabled (Remote Check)	10.0 (High)	80%	127.0.0.34	445/tcp	Thu Mar 23 16:33:27 2017
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	127.0.0.10	445/tcp	Thu Mar 23 16:33:27 2017
SMBv1 enabled (Remote Check)	10.0 (High)	80%	127.0.0.25	445/tcp	Thu Mar 23 16:33:27 2017

<http://openvas.org/>



CVE List Board

CNA
About
News & Blog

NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search

Search CVE List Download CVE Data Feeds Request CVE
IDs Update a CVE Entry

TOTAL CVE Entries: 115184

HOME > CVE > SEARCH RESULTS

Search Results

There are 51 CVE entries that match your search.

Name	Description
CVE-2019-1698	A vulnerability in the web-based user interface of Cisco Internet of Things Field Network Director (IoT-FND) Software could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by importing a crafted XML file with malicious entries, which could allow the attacker to read files within the affected application. Versions prior to 4.4(0.26) are affected.
CVE-2019-1644	A vulnerability in the UDP protocol implementation for Cisco IoT Field Network Director (IoT-FND) could allow an unauthenticated, remote attacker to exhaust system resources, resulting in a denial of service (DoS) condition. The vulnerability is due to improper resource management for UDP ingress packets. An attacker could exploit this vulnerability by sending a high rate of UDP packets to an affected system within a short period of time. A successful exploit could allow the attacker to exhaust available system resources, resulting in a DoS condition.
CVE-2019-0741	An information disclosure vulnerability exists in the way Azure IoT Java SDK logs sensitive information, aka 'Azure IoT Java SDK Information Disclosure Vulnerability'.
CVE-2019-0729	An Elevation of Privilege vulnerability exists in the way Azure IoT Java SDK generates symmetric keys for encryption, allowing an attacker to predict the randomness of the key, aka 'Azure IoT Java SDK Elevation of Privilege Vulnerability'.

<https://cve.mitre.org/>

Internet stvari

I3 Insecure Ecosystem Interfaces

- Objedinjene 3 top ranjivosti iz 2014:
 - IoT uređaji tipično komuniciraju s poslužiteljem – nesigurna sučelja weba (ex. I1)
 - Zapravo OWASP web top 10 (prethodno predavanje)
 - Možemo li provaliti sučelje na poslužitelju i doći do podataka s uređaja?
 - Usluge često imaju mobilne aplikacije za pregled podataka i upravljanje uređajima (npr. kamere) (ex. I7)
 - Vrlo slično OWASP top 10 mobilnih ranjivosti (prethodno predavanje)
 - Možemo li preko aplikacije ii sučelja za aplikaciju na uređaju preuzeti kontrolu?
 - Tipično uređaje IoT kontroliramo / agregiramo podatke putem sučelja u oblaku (ex. I6)
 - Ponovno, vrlo slično ex. I1 – poslužitelji weba i njihova sučelja

I4 Lack of Secure Update Mechanism

- Ažuriranje programske podrške je uvijek nužno
 - Pronađene ranjivosti → zakrpe (npr. napadači - diff!)
- Problem može biti i “nesigurno” ažuriranje
 - Autentifikacija poslužitelja - automatizirano ažuriranje sa preuzetog “update servera”
 - NotPetya – Ukrajina, brave s Airbnb...
 - Prijenos ažuriranja mora biti šifriran
 - Ažurirani software/firmware ne smije sadržavati “hardkodirane” autentifikacijske podatke! (npr. kako do ključeva iz hardvera?)
- Osnovne provjere:
 - Može li se software/firmware uređaja uopće ažurirati?

I5 Use of Insecure or Outdated Components

- Korištenje zastarjelih ili nesigurnih komponenti
 - Programske knjižnice, radni okviri...
 - Nesigurna dorada funkcija operacijskog sustava
 - Nesigurno sklopolje?
- Osnovne provjere:
 - Pobrojati što se sve koristi
 - Provjeriti je li sve ažurirano
 - Sličan princip kao i kod ranjivosti weba...

I6 Insufficient Privacy Protection

- Uređaji IoT mogu skupljati osobne podatke
 - Kamere, mikrofoni, medicinski podaci...
- Problem: kompromitacija takvih podataka koje napadači tipično koriste za daljnje napade
 - Phishing, spear-phishing, ucjene, lažno predstavljanje...
- Osnovne provjere
 - Kakve sve podatke uređaj IoT skuplja (i je li to nužno)?
 - Što se radi s tim podacima - gdje se i kako obrađuju/šalju?
 - jesu li anonimizirani u nekoj mjeri?
 - Domena GDPR-a
 - Posljedica zapravo svih ranjivosti I1-I10
- Npr. Amazon Echo – "prisluškivanje" za poboljšanje usluge?

I7 Insecure Data Transfer and Storage

- Česta ranjivost općenito, donekle smanjena posljednjih godina
- Nepostojanje šifriranja prometa na transportnom sloju
 - Sva komunikacija je lako čitljiva metodama "sniffanja" (npr. Wireshark)
- Nepostojanje šifriranja podataka "u mirovanju" – novost!
- Potrebno je ispravno koristiti infrastrukturu PKI, ključeve i mehanizme
- Osnovne provjere:
 - Analiza prometa kako bi se utvrdilo je li dio ili sav promet šifriran
 - Ako se koristi TLS provjeriti da se koristi ispravno
 - Dosta postojećih problema s neispravnim korištenjem (npr. SSLstrip)
 - Provjera korištenih algoritama i ključeva – jesu li zastarjeli?
 - Nove preporuke svakih nekoliko godina
- ESP8266 npr.: <https://hackaday.com/2017/06/20/practical-iot-cryptography-on-the-espressif-esp8266/>

I8 Lack of Device Management

- Upravljanje i nadzor IoT uređaja
- Znamo li gdje su, u kojem su stanju, rade li ispravno, rade li uopće...
- Problem sa zamjenom / isključivanjem uređaja?
 - Npr. smart dust problem
- Problem “rogue node” – kako detektirati lažni uređaj?
- Kao Logging and monitoring kod web-aplikacija

I9 Insecure Default Settings

- Tko je kriv za MIRAI botnet? (korišteni su *default* računi!)
- Može li se mijenjati sigurnosne postavke uređaja?
 - Mora li ih se mijenjati? (MIRAI!)
 - Što ako postane prekompleksno – korisnici očekuju PnP! (loše)
- Osnovne provjere:
 - Ako već proizvođač ne forsira jake lozinke, mogu li ih sam forsirati na administratorskom sučelju?
 - Ima li mogućnosti povećavanja sigurnosti putem sučelja:
 - Logiranje svih akcija u sustavu (bitno za napade iznutra!)
 - Upozorenja u slučaju incidenata (mail, SMS, alarm)?
 - Definiranje korisničkih uloga
- https://www.owasp.org/index.php/Top_10_2014-I8_Insufficient_Security_Configurability



I10 Lack of Physical Hardening

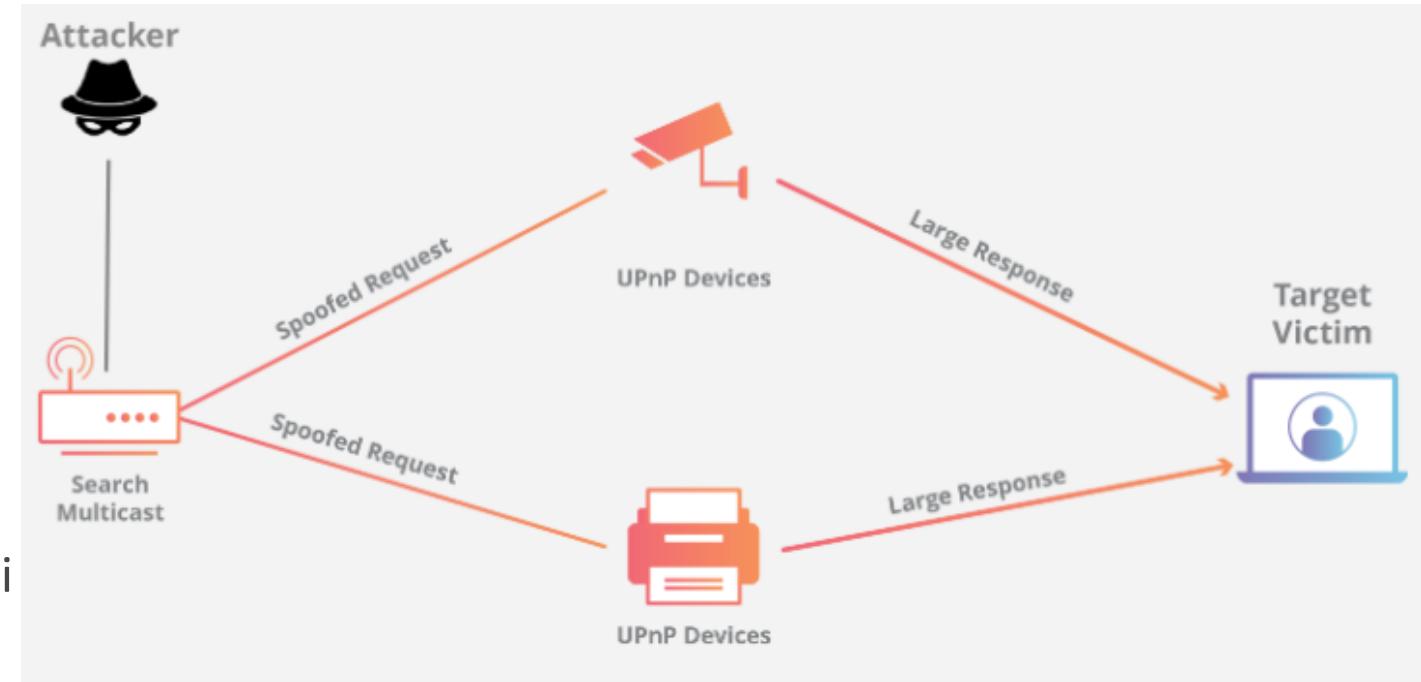
- Što napadač može napraviti ako ima fizički pristup uređaju?
 - Kako do ključeva/lozinki iz sklopolja? (prošli *slide*)
 - Pristup podacima (npr. očitanja) pohranjenim na memorijskoj kartici
 - Pristup USB-u i sličnim priključcima (npr. PoisonTap)?
- Osnovne provjere:
 - Mogu li jednostavno "otvoriti" uređaj? Postoji li detekcija?
 - Mogu li se spojiti na ulaze (npr. USB) namijenjene konfiguraciji uređaja?
 - Mogu li programski onemogućiti lokalno spajanje na uređaj?
 - Jesu li pohranjeni podaci šifrirani?
- https://www.owasp.org/index.php/Top_10_2014-I10_Poor_Physical_Security

Kako se štititi?

- Shvatiti zašto postoje ranjivosti (...)
- Za svaku ranjivost OWASP ima preporuke (poveznice)
- Smjernice za razvijatelje
 - Kako razvijati, što omogućiti, na što paziti?
- Smjernice za korisnike
 - Kako osigurati uređaj / sustav?
 - *Default* je uobičajeno jednostavan i nesiguran!
 - Tko je kriv u slučaju zlouporaba?
- Sigurnost je složena i traži puno znanja na svim “slojevima”
 - Jedna ranjivost može kompromitirati cijeli sustav!

Uređaji IoT kao sredstvo za DDoS? – npr. SSDP DDoS

- "amplification" napad
- UPnP (Universal Plug'n'Play) uređaji (PS4, Smart TV, kamere...)
 - Koriste SSDP (Simple Service Discovery Protocol) za objavu slanjem paketa na multicast adresu – koriste UDP!
 - Nakon objave računala ih mogu zatražiti karakteristike / usluge → pojačanje!
- Napadač lažira IP adresu žrtve i zatraži karakteristike od velikog broja UPnP uređaja...



<https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/>

Neki korisni resursi...

- Smjernice GSMA IoT Security
 - 85 preporuka za siguran dizajn IoT sustava, uređaja...
 - Ranjivosti, modeli napada i procjena rizika za svaki slučaj
 - <https://www.gsma.com/iot/iot-security/iot-security-guidelines/>
- SHODAN (<https://www.shodan.io/>)
 - Google za IoT uređaje
 - Pretraga uređaja
 - Pretraga pronađenih ranjivosti
 - Koristiti kao prvi korak napada (probe)?

SHODAN

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
25

TOP COUNTRIES



Croatia 25

TOP CITIES

Zagreb	16
Karlovac	3
Dubrovnik	2

TOP SERVICES

2002	7
Telnet	7
HTTPS	5
264	3
HTTP	1

TOP ORGANIZATIONS

VIPnet d.o.o.	11
Croatian Academic and Research ...	8
T-Mobile Croatia	2
Metronet telekomunikacije d.d.	2
POSLuH d.o.o., za informaticke usl... <td>1</td>	1

193.198.162.131
Croatian Academic and Research Network
Added on 2019-04-13 13:14:39 GMT
Croatia, Zagreb

Studentski centar u Zagrebu
University of Zagreb

Studom
Stjepan Radic
Zagreb, Croatia

Authorized access only !!!

193.198.162.139
Croatian Academic and Research Network
Added on 2019-04-16 20:16:06 GMT
Croatia, Zagreb

|
|
| Studenski centar
| Sveucilista u Zagrebu
|
| ...
|

83.139.115.146 
dh115-146.xnet.hr
VIPnet d.o.o.
Added on 2019-04-17 01:18:41 GMT
Croatia, Zagreb

HTTP/1.1 200 OK
Date: Wed, 17 Apr 2019 01:18:41 GMT
Server: Apache
Last-Modified: Mon, 02 Sep 2013 12:31:25 GMT
ETag: "90dd04-249-c025c140"
Accept-Ranges: bytes
Content-Length: 585
Content-Type: text/html

Internet stvari
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/...

Za one koji žele znati više

- <https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>
- [https://www.owasp.org/index.php/OWASP Internet of Things Project#tab>Main](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main)
- <https://www.gsma.com/iot/iot-security/iot-security-guidelines/>
- <https://www.shodan.io>