# Pregled razvoja i primjene bežičnih komunikacijskih tehnologija u području koncepta IoT

**Marinović, Ante**

# SVEUČILIŠTE U ZAGREBU

# FAKULTET PROMETNIH ZNANOSTI

**Ante Marinović**


# PREGLED RAZVOJA I PRIMJENE BEŽIČNIH KOMUNIKACIJSKIH TEHNOLOGIJA U PODRUČJU KONCEPTA IOT

**ZAVRŠNI RAD**


**Zagreb, 2021.**

**SVEUČILIŠTE U ZAGREBU**
**FAKULTET PROMETNIH ZNANOSTI**
ODBOR ZA ZAVRŠNI RAD

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Informacije i komunikacije**

# ZAVRŠNI ZADATAK br. 6137

Pristupnik: **Ante Marinović (0135250963)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Pregled razvoja i primjene bežičnih komunikacijskih tehnologija u području koncepta IoT**

Opis zadatka:

U završnom radu potrebno je definirati pojam koncepta Internet stvari i dati osvrt na područja primjene ovog koncepta. Zatim je potrebno analizirati bežične komunikacijske tehnologije primjenjive u konceptu IoT kao i sigurnosne aspekte analiziranih tehnologija. Završno, potrebno je utvrditi i istaknuti trenutne i nadolazeće komunikacijske izazove u konceptu IoT.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

# ZAVRŠNI RAD

# PREGLED RAZVOJA I PRIMJENE BEŽIČNIH KOMUNIKACIJSKIH TEHNOLOGIJA U PODRUČJU KONCEPTA IOT

# AN OVERVIEW OF THE DEVELOPMENT AND APPLICATION OF WIRELESS COMMUNICATION TECHOLOGIES IN THE FIELD OF IOT CONCEPT

Mentor: dr. sc. Ivan Cvitić

Student: Ante Marinović

JMBAG: 0135250963

Zagreb, rujan 2021.

# SAŽETAK

Koncept interneta stvari u stalnom je razvoju s ciljem poboljšanja kvalitete života. Osnovni primjer takvih uređaja može se vidjeti kod raznih kućanskih aparata, rasvjete ili drugih uređaja u brojnim pametnim kućanstvima. Osim toga, postoje i druga razna područja primjene internet stvari poput pametnog grada, zdravstva, transporta, okoliša, energije i proizvodnje. U ovom završnom radu definiran je pojam koncepta internet stvari i dati osvrt na područja primjene ovog koncepta. Analizirane su najznačajnije bežične komunikacijske tehnologije primjenjive u spomenutom konceptu, koje smo podijelili na tehnologije dugog i kratkog dometa. Ključni sigurnosni problemi unutar IoT sustava su povjerljivi podaci i provjera identiteta. Završno su istaknuti najvažniji izazovi komunikacije u konceptu IoT, od kojih je ključan izazov sigurnost.



**Ključne riječi**: internet stvari (IoT), pametni uređaji, pametan grad, komunikacijske tehnologije, sigurnost, podaci, identitet



# SUMMARY

The concept of the Internet of Things is constantly evolving with the aim of improving the quality of life. A basic example of such devices can be seen in various household appliances, lighting or other devices in many smart households. In addition, there are other various areas of application of the Internet of Things like smart city, healthcare, transportation, environment, energy and manufacturing. In this final paper, the concept of the Internet of Things concept is defined and a review of the areas of application of this concept is given. The most significant wireless communication technologies applicable in the mentioned concept are analyzed, which we have divided into long-range and short-range technologies. Key security issues within the IoT system are confidential data and authentication. Finally, the most important communication challenges in the IoT concept are highlighted, of which the key challenge is security.



**Keywords:** internet of things (IoT), smart devices, smart city, communication technologies, security, data, identity

**SADRŽAJ**


1. Uvod ... 1
2. Koncept Internet stvari ... 2
   2.1. Arhitektura koncepta IoT ... 2
      2.1.1. Sloj objekata ... 3
      2.1.2. Sloj apstrakcije objekta ... 3
      2.1.3. Sloj upravljanja uslugama ... 4
      2.1.4. Aplikacijski sloj ... 4
      2.1.5. Poslovni sloj ... 4
   2.2. IoT elementi ... 4
      2.2.1. Identifikacija ... 5
      2.2.2. Senzoriranje ... 5
      2.2.3. Komunikacija ... 5
      2.2.4. Procesiranje ... 6
      2.2.5. Usluge ... 6
      2.2.6. Semantika ... 7
      2.2.7. Usporedba elemenata ... 7
3. Područja primjene koncepta Internet stvari ... 8
   3.1. Pametni grad ... 10
   3.2. Pametne zgrade ... 11
   3.3. Pametno zdravstvo ... 13
   3.4. Pametni okoliš ... 13
   3.5. Pametna energija ... 14
   3.6. Pametni transport i mobilnost ... 15
   3.7. Pametna proizvodnja ... 15
4. Bežične komunikacijske tehnologije korištene u konceptu IoT ... 17
   4.1. Mreže kratkog dometa ... 17
   4.2. Mreže dugog dometa ... 18
   4.3. Usporedba tehnologija ... 19
   4.4. Zajednički protokoli ... 20
      4.4.1. Aplikacijski protokoli ... 21
      4.4.2. Protokoli za otkrivanje usluge ... 22
      4.4.3. Infrastrukturni protokoli ... 23
      4.4.4. Ostali utjecajni protokoli ... 25

5. Sigurnost bežičnih komunikacijskih tehnologija ..... 27
6. Izazovi komunikacije u konceptu IoT ..... 30
7. Zaključak ..... 32
Literatura ..... 33
Popis slika ..... 36
Popis tablica ..... 36
Popis grafikona ..... 36

# 1. Uvod

Rastući broj uređaja povezuje se na Internet razvijajući ideju interneta stvari (engl. *Internet of Things, IoT*). Osnovi primjer takvih uređaja može se vidjeti kod termostata, rasvjete ili drugih kontrolnih uređaja u brojnim 'pametnim' kućanstvima. Naravno, postoje i druga područja u kojima IoT igra važnu ulogu kako bi se poboljšala kvaliteta života. Samo neka od njih su transport, zdravstvo, industrijska automatizacija itd. IoT daje svakodnevnim objektima mogućnost osjeta, vida i sluha, povezuje ih i omogućuje njihovu razmjenu informacija. Internet stvari pretvara obične uređaje u 'pametne' iskorištavajući njihove potencijale kroz ugradbene sustave, komunikacijske tehnologije, senzorske mreže, internetske protokole i aplikacije. Pretpostavlja se da će IoT s vremenom biti uključen u većinu kućanstava i poslovnih institucija s idejom poboljšanja života i rastom svjetske ekonomije. Na primjer, 'pametna' kućanstva će omogućiti osobama koje u njima žive automatsko otvaranje garaže, pripremanje kave, klimatizaciju itd. Kako bi se dosegnuo takav potencijal, potrebno je uskladiti podjednak rast dostupnih tehnologija i inovacija zajedno s tržištem i potrebom potrošača.

Tema završnog rada je Pregled razvoja i primjene bežičnih komunikacijskih tehnologija u području koncepta IoT. Rad se sastoji od sedam poglavlja:

1. Uvod
2. Koncept Internet svari
3. Područja primjene koncepta Internet stvari
4. Bežične komunikacijske tehnologije korištene u konceptu IoT
5. Sigurnost bežičnih komunikacijskih tehnologija
6. Izazovi komunikacije u konceptu IoT
7. Zaključak

Cilj ovog rada je definiranje pojma koncepta internet stvari te davanje osvrta na područja primjene ovog koncepta. U drugom poglavlju prikazani su načini izvedbe arhitekture, kao i elementi interneta svari, zatim u trećem poglavlju predstavljena su različita područja primjene navedenog koncepta. U četvrtom poglavlju nabrojene su te ukratko opisane neke od bežičnih komunikacijskih tehnologija korištene konceptu IoT, kroz peto poglavlje prikazan je osvrt na sigurnost bežičnih komunikacijskih tehnologija te su kroz šesto poglavlje predstavljeni glavni izazovi komunikacije odnosno problemi koje bi se trebalo rješavati u budućnosti.

# 2. Koncept Internet stvari

IoT je sustav povezivanja svih uređaja putem interneta. IoT se sastoji od dva pojma: Internet i stvar. Pojam internet je globalni sustav računalnih mreža i krajnjih uređaja. Oni za komunikaciju koriste standardizirani internet protokol stog (TCP/IP). Pojam stvari su fizički objekti poput svakodnevno korištenih elektroničkih uređaja, napredni tehnološki proizvodi, odjeća, namještaj i drugo [1].

## 2.1. Arhitektura koncepta IoT

IoT bi trebao biti sposoban povezati milijarde ili bilijune heterogenih objekata putem Interneta, tako da postoji kritična potreba za fleksibilnom i slojevitom arhitekturom. Sve veći broj predloženih arhitektura se još nije približio referentnom modelu. Međutim, postoje neki projekti poput IoT-A (engl. *Internet of Things-Arhitecture*, arhitektura Internet stvari), koji pokušavaju dizajnirati zajedničku arhitekturu temeljenu na analizi potreba istraživača i industrije. Iz baze predloženih modela, osnovni model je troslojna arhitektura. U novijoj literaturi predloženi su neki drugi modeli koji dodavaju više apstrakcija IoT arhitekturi [2]. Tablica 1 prikazuje neke uobičajene arhitekture među kojima je od velike važnosti petoslojni model.

**Tablica 1.** Prikaz IoT arhitekture

<table>
<tr><td rowspan="3">Aplikacijski sloj</td><td colspan="2">Aplikacijski sloj</td><td>Aplikacije</td><td>Poslovni sloj</td></tr>
<tr><td colspan="2">Srednjebazni sloj</td><td>Sastav usluge</td><td>Aplikacijski sloj</td></tr>
<tr><td colspan="2">Koordinacijski sloj</td><td>Upravljanje uslugama</td><td>Upravljanje uslugama</td></tr>
<tr><td>Mrežni sloj</td><td colspan="2">Sloj jezgrene mreže</td><td>Apstrakcija objekta</td><td>Apstrakcija objekta</td></tr>
<tr><td rowspan="2">Percepcijski sloj</td><td rowspan="2">Samopostojani aplikacijski sloj</td><td>Pristupni sloj</td><td rowspan="2">Objekti</td><td rowspan="2">Objekti</td></tr>
<tr><td>EDGE tehnologija</td></tr>
</table>

Izvor: [2]

Prvi stupac prikazuje troslojni model, koji predstavlja elementarnu arhitekturu koja je definirana početnim istraživanjima. Sastoji se od percepcijskog, mrežnog i aplikacijskog sloja. Senzorske tehnologije, RFID i druge tehnologije ključne su u percepcijskom sloju, čija je svrha prikupljanje informacija. Svrha mrežnog sloja, koji predstavlja jezgru komunikacije koncepta IoT, je prijenos informacija. Informacije koje su prikupljene na percepcijskom sloju

prenose se na aplikacijski sloj i obrnuto. Zadaća aplikacijskog sloja je integracija informacija i njihova isporuka krajnjim korisnicima. Zbog iznimno brzog razvoja internet stvari, troslojna arhitektura postaje nedovoljna te se zamjenjuje s petoslojnom arhitekturom [1].

Drugi stupac prikazuje arhitekturu baziranu na srednje-baznom (engl. *Middle-ware*) modelu, dok treći stupac prikazuje arhitekturu baziranu na SOA modelu, tj. uslužno-orijentirana arhitektura (engl. *Service-oriented architecture*) [2]. Jasna međusobna komunikacija postaje imperativ za pružatelje i tražitelje usluga kod primjene SOA arhitekture, neovisno o heterogenoj prirodi informacijskih struktura. Usvajanje SOA arhitekture omogućava višestruku primjenu istih softverskih i hardverskih komponenata te dekompoziciju kompleksnih sustava jer nije potrebna primjena određenih tehnologija za implementaciju usluga [1].

Posljednji stupac prikazuje petoslojni model, koji se sastoji od [2]:

- Sloja objekata (engl. *Objects Layer*),
- Sloja apstrakcije objekta (engl. *Object Abstraction Layer*),
- Sloja upravljanja uslugama (engl. *Service Management Layer*),
- Aplikacijskog sloja (engl. *Application Layer*) i
- Poslovnog sloja (engl. *Business Layer*).

### 2.1.1. Sloj objekata

Prvi sloj, objektni ili percepcijski sloj, predstavlja fizičke senzore od strane IoT kojima je cilj prikupiti i obraditi informacije. Ovaj sloj uključuje senzore i pokretače za obavljanje različitih funkcija, poput upita za lokaciju, određivanje temperature, težinu, kretanje, vibracije, akceleracije, vlažnost, itd. Takav sloj treba koristiti standardizirane *plug-and-play* mehanizme za konfiguraciju heterogenih objekata. Percepcijski sloj digitalizira i prenosi podatke na sloj apstrakcije objekta kroz sigurnosne kanale. Velike količine podataka stvorene od strane IoT pokreću se na ovom sloju [2].

### 2.1.2. Sloj apstrakcije objekta

Drugi sloj po redu, sloj apstrakcije objekta prenosi podatke koje proizvodi prvi sloj prema trećem sloju, odnosno prema sloju upravljanja uslugama putem sigurnosnih kanala. Podaci se mogu prenositi putem različitih tehnologija poput: identifikacije radio frekvencije - RFID (engl. *Radio-frequency identification*), treće generacije mobilnih mreža - 3G (engl. *Third generation*), globalnog sustava za mobilne komunikacije - GSM (engl. *Global System*

*for Mobile Communications*), univerzalnog mobilnog telekomunikacijskog sustava - UMTS (engl. *Universal Mobile Telecommunications System*), tehnologije bežičnog umrežavanja - WiFi (engl. *wireless networking technology*), Bluetooth-a, ZigBee, i dr. Nadalje, ostale funkcije poput računarstva u oblaku (engl. *Cloud computing*) i procesa upravljanja podacima se obrađuju na ovom sloju [2].

### 2.1.3. Sloj upravljanja uslugama

Upravljanje uslugama ili srednje-bazni softver spaja uslugu s podnositeljem zahtjeva zasnovanim na adresi i imenu. Ovaj sloj omogućava programima aplikacije IoT rad s heterogenim objektima bez obzira na specifičnost računalne (hardverske) platforme. Ovaj sloj također obrađuje primljene podatke, donosi odluke i šalje tražene usluge mrežnim žičnim protokolima [2].

### 2.1.4. Aplikacijski sloj

Aplikacijski sloj pruža klijentima tražene usluge. Ovaj sloj može npr. osigurati mjerenje temperature i vlage u zraku, klijentima koji su zatražili taj podatak. Važnost ovoga sloja za IoT sastoji se u njegovoj sposobnosti pružanja visokokvalitetnih pametnih usluga koje zadovoljavaju potrebe klijenata. On pokriva brojna vertikalna tržišta poput: pametnog doma, pametne kuće, prijevoza, industrijske automatizacije i pametne zdravstvene skrbi [2].

### 2.1.5. Poslovni sloj

Poslovni sloj upravlja cjelokupnim sustavom aktivnosti i usluga IoT-a. Zadaća ovoga sloja je izgraditi poslovni model, grafikone, dijagram toka i sl. na osnovi podataka dobivenih od aplikacijskog sloja. Ovaj sloj je također predviđen da dizajnira, analizira, provodi, procjenjuje, nadzire i razvija elemente povezane sa sustavom IoT-a. Poslovni sloj omogućava pružanje potpore u procesu odlučivanja na osnovi analize velikih podataka. U ovome sloju moguć je također nadzor i upravljanje četirima nižim slojevima. Ovaj sloj uspoređuje ostvareni rezultat (engl. *output*) svakog sloja s očekivanim rezultatom kako bi se poboljšala usluga i zaštitila privatnost korisnika [2].

## 2.2. IoT elementi

Razumijevanje blokova odnosno sastavnih elemenata IoT, pomaže u stjecanju boljeg uvida u njegovo stvarno značenje i funkcioniranje. Slika 2. prikazuje šest glavnih elemenata potrebnih za funkcioniranje IoT.


**Slika 1**. IoT elementi

Izvor: [2].

### 2.2.1. Identifikacija

Identifikacija (engl. *Identification*) je ključna za IoT radi imenovanja i povezivanja usluga s njihovim zahtjevima. Dostupne su brojne identifikacijske metode poput: elektroničkog proizvodnog koda (EPC) (engl. *Electronic product code*) i neograničenog/neprekidnog koda - uCode (engl. *Ubiquitous code*). Određivanje adresiranja objekata kod IoT je ključno za razlikovanje identifikacije (ID) objekta i njegove adrese. ID objekta se odnosi na njegovo ime, kao npr. "T1" za određeni temperaturni senzor, a adresa objekta odnosi se na njegovu adresu u sklopu komunikacijske mreže. Pored toga, identifikacija objekata IoT uključuje IPv6, IPv4 i 6LoWPAN. Razlikovanje identifikacije objekta i njegove adrese je ključno jer identifikacijske metode nisu jedinstvene u cijelome svijetu, tako da adresiranje pomaže u jedinstvenoj identifikaciji objekata. Identifikacijske metode se koriste za jasan identitet svakog objekta u sklopu mreže [2].

### 2.2.2. Senzoriranje

Drugi elemenat po redu, IoT senzoriranje (engl. *Sensing*) podrazumijeva skupljanje podataka iz povezanih objekata u sklopu mreže i vraćanje istih u pohranu, u bazu podataka ili u oblak (engl. *Cloud*). Prikupljeni podaci se analiziraju kako bi se poduzele posebne radnje vezane za tražene usluge. Senzori IoT mogu biti pametni senzori, aktuatori ili nosivi senzorski uređaji. Tako npr. tvrtke poput Wemo, Revolv and SmartThings nude pametna čvorišta i mobilne aplikacije koje ljudima omogućuju  nadzor i kontrolu tisuća pametnih uređaja u zgradama koristeći pametne telefone [2].

### 2.2.3. Komunikacija

IoT komunikacijske tehnologije povezuju heterogene objekte kako bi pružili specifične pametne usluge. IoT čvorovi u radu koriste smanjenu energiju u prisutnosti bučnih komunikacijskih veza. Primjeri komunikacijskih protokola korištenih za IoT su WiFi, Bluetooth, IEEE 802.15.4, Z-wave i LTE-A (engl. *Long Term Evolution-Advanced*). Također

se koriste i neke posebne komunikacijske tehnologije, kao što su: RFID i komunikacija bliskog polja - NFC (engl. *Near field communication*) [2].

### 2.2.4. Procesiranje

Kod elementa procesiranje (engl. *Computation*), procesne jedinice (npr. mikroprocesori) i softverske aplikacije su 'mozak' i računalna sposobnost IoT. Razvijene su razne hardverske platforme za upravljanje aplikacijama IoT poput: Arduino-a, UDOO-a, FriendlyARM, Intel Galileo, Raspberry PI, itd…

Također, koriste se i mnoge softverske platforme za pružanje funkcija IoT. Operativni sustavi su među navedenim platformama od vitalne važnosti jer oni rade kroz cijelo vrijeme aktivacije uređaja [2].

### 2.2.5. Usluge

Sljedeći elemenat po redu, usluge (engl. *Services*) mogu se podijeliti u četiri kategorije:

- Identitetski povezane usluge (engl. *Identity-related Services*),
- Usluge prikupljanja informacija (engl. *Information Aggregation Services*),
- Usluge koje potiču svijest o suradnji (engl. *Collaborative-Aware Services*) i
- Neograničene usluge (engl. *Ubiquitous Services*).

Identitetski povezane usluge su osnovne i najvažnije usluge koje se koriste u ostalim vrstama usluga. Svaka aplikacija koja treba objekte iz stvarnoga svijeta prenijeti u virtualni svijet mora te objekte identificirati. Usluga prikupljanja informacija prikuplja i sažima neobrađena senzorska mjerenja koja treba obraditi i prenijeti/poslati u aplikaciju IoT. Usluge koje potiču svijest o suradnji djeluju iznad usluge prikupljanja informacija i koriste dobivene podatke u svrhu donošenja odluka i adekvatne reakcije. Svrha neograničenih usluga je osiguranje CAS-a u svako doba, na svakome mjestu. Krajnji cilj svih aplikacija IoT je dostići stupanj neograničenih usluga. Ovaj cilj, međutim, nije lako dostići zbog raznih poteškoća i izazova. Većina postojećih aplikacija osigurava usluge povezane s identitetom.

Pametna briga o zdravlju i pametne mreže spadaju u kategoriju prikupljanja informacija, dok su usluge pametnoga doma, pametnih zgrada, inteligentnog transportnog sustava - ITS i industrijske automatizacije bliže kategoriji svijesti o suradnji [2,3].

### 2.2.6. Semantika

Posljednji elemenat po redu, semantika (engl. *Semantics*) se u IoT odnosi na sposobnost pametnog izdvajanja znanja pomoću različitih strojeva u svrhu pružanja traženih usluga. Izdvajanje znanja podrazumijeva otkrivanje i korištenje resursa i modeliranje podataka. Ono također uključuje prepoznavanje i analiziranje podataka kako bi se donijela prava odluka u pružanju prave usluge. Semantika zapravo predstavlja 'mozak' IoT, tako što šalje zahtjeve pravome resursu. Ovaj postupak podržavaju tehnologije semantičke mreže kao što su: okvir opisa resursa - RDF (engl. *Resource Description Framework*) i Ontološki jezik web-a - OWL (engl. *Web Ontology Language*) [2].

### 2.2.7. Usporedba elemenata

U tablici 2. prikazani su spomenuti elementi i tehnologije koje im pripadaju. Za element identifikacije imenovanje je EPC i uCode, a adresiranju pripadaju verzije internet protokola: IPv4 i IPv6. Pametni senzori, aktuatori ili nosivi senzorski uređaji pripadaju elementu senzoriranje. Primjeri protokola komunikacijskog elementa su RFID, NFC, Bluetooth, WiFi i ostali navedeni protokoli. Zatim, elemenat procesiranje možemo prikazati u dva dijela: hardverski dio kojeg predstavljaju pametne stvari, Arduino, Raspberry PI i drugi pametni uređaji i softverski dio koji predstavlja operacijski sustav za različite sustave poput Contiki, TinyOS, Android i drugih. Sljdeći elemenat, usluge, kako je navedeno u tablici, možemo podijeliti u četiri kategorije. Posljednji i jako bitan elemenat kojeg podržavaju tehnologije RDF i OWL je semantika.

**Tablica 2.** Prikaz IoT elemenata i tehnologija

| **IoT elementi** | | **Primjeri** |
|---|---|---|
| identifikacija | imenovanje | EPC, uCode |
| | adresiranje | IPv4, IPv6 |
| senzoriranje | | pametni senzori, aktuatori ili nosivi senzorski uređaji |
| komunikacija | | RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, LTE-A |
| procesiranje | hardver | pametne stvari, Arduino, Intel Galileo, Raspberry PI, pametni uređaji |
| | softver | OS (Contiki, TinyOS, LiteOS, Riot OS, Android) |
| usluge | | identitetski povezane usluge, usluge prikupljanja informacija, usluge koje potiču svijest o suradnji, neograničene usluge |
| semantika | | RDF, OWL |

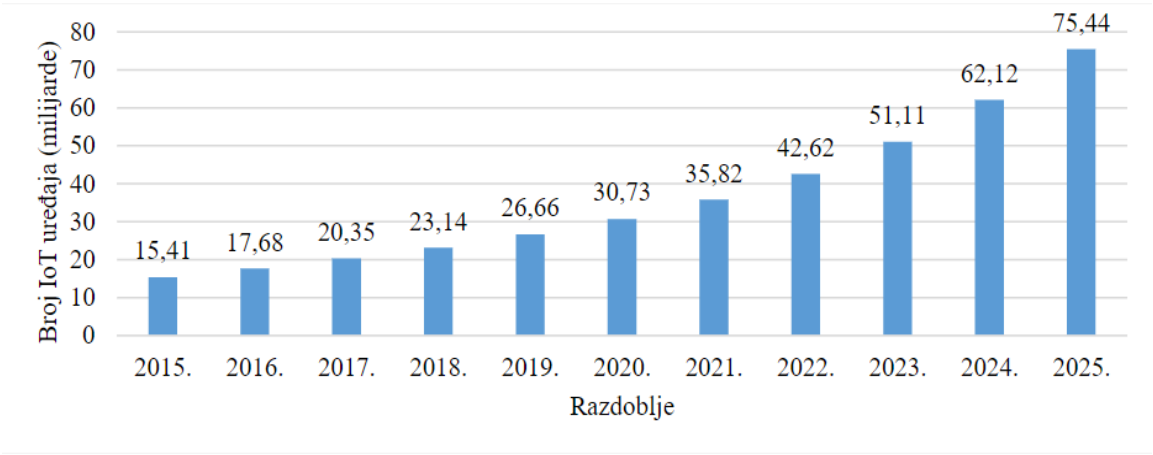
Izvor: [2].

# 3. Područja primjene koncepta Internet stvari

Ključni dio koncepta internet stvari je M2M (engl. *Machine-to-machine*). M2M je direktna komunikacija između uređaja koji koriste žične ili bežične komunikacijske kanale. Sastoji se od manjih uređaja koji očitavaju informacije iz okoline i šalje ih do glavne platforme koja koristi softver pomoću kojeg te informacije obrađuje te mijenja uvjete izvođenja nekog zadatka (npr. industrijski pogoni, gradilišta, skladišta i dr.) [4].

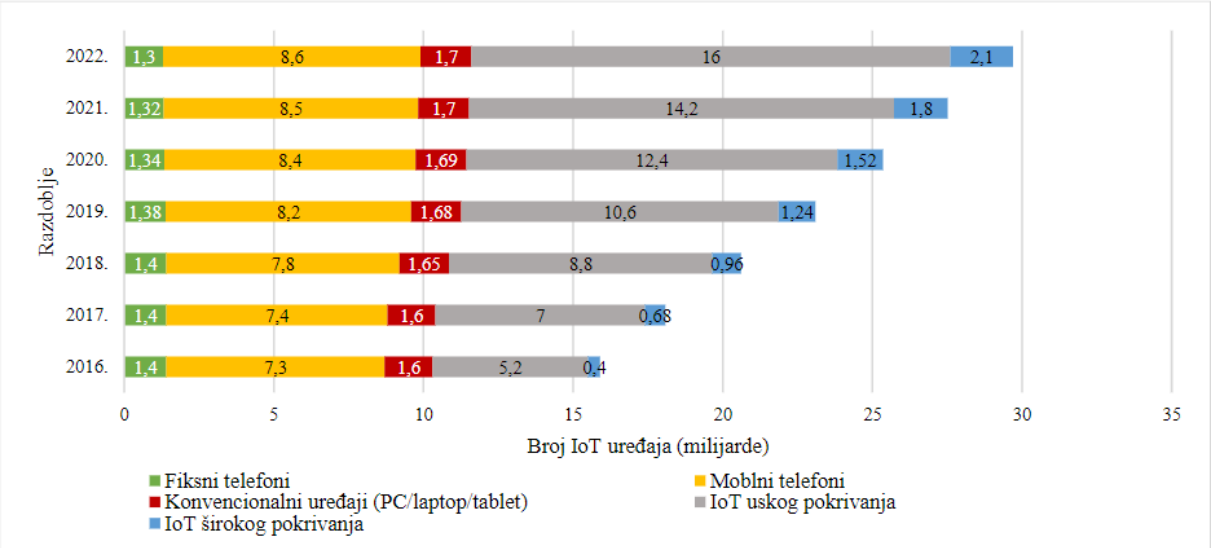
Broj uređaja povezanih na internet raste eksponencijalno a samim time i mrežni promet. U većini situacija to podrazumijeva niskoenergetske uređaje na baterije koji šalju i primaju poruke preko ograničenih mreža, za razliku od tradicionalnih komunikacijskih kanala koji su ovisili o ljudskom djelovanju [4]. Statistički pokazatelji broja IoT uređaja u razdoblju od 2015. do 2025. godine, prikazani su na grafikonu 1. Do kraja ove godine predviđa se 35 millijardi IoT uređaja, dok se do kraja 2025. godine predviđa golemih 75 milijardi IoT uređaja.

Grafikon 1. Predikcija ukupnog broja IoT uređaja do 2025.(globalno), [1]




Podaci koji se odnose na zastupljenost pojedine kategorije povezanih uređaja, prema globalnim pokazateljima tvrtke Ericsson, vidljiva je dominacija IoT uređaja u odnosu na ostale mobilne uređaje [1]. Grafikon 2. prikazuje broj povezanih uređaja prema kategorijama u razdoblju od 2016. do 2022 godine.

Grafikon 2. Broj povezanih uređaja prema kategorijama, [1]




Razumijevanje karakteristika prometa generiranog od strane korisnika mreže ključan je prvi korak u dizajniranju mreža. Što se tehnologija bolje podudara sa zahtjevima primjene IoT, to bolje koristi resurse, koji su ograničeni. Dobro poznavanje karakteristika prometa omogućava stvaranje novih poslovnih prilika, zato jer krajnji korisnici mogu točnije procijeniti približne troškove mrežne komunikacije i usporediti ih s vrijednosti dobivenih informacija, a mrežni operateri mogu pronaći nova tržišta za pružanje svojih usluga. Karakteristike prometa otkrivaju prednosti korištenja koncepta IoT kao i brojne prepreke u širenju IoT globalno. Razumijevanje ovih problema može poboljšati trenutna rješenja i ubrzati cijeli proces izvedbe. Domene primjene IoT se sastoje od velikog broja usluga koje mogu imati jako raznovrsne karakteristike prometa i zato moramo svaku uslugu gledati pojedinačno, stoga je važno napomenuti da različita rješenja koja teže pružanju iste usluge mogu imati malo drugačiju konfiguraciju dok osnovni principi ostaju isti [5].

Ovo poglavlje pružiti će pregled primjene koncepta IoT u sljedećim područjima:

- Pametnog grada,
- Pametnih zgrada,
- Pametnog zdravstva,
- Pametnog okoliša,
- Pametne energije,
- Pametnog transporta i mobilnosti i
- Pametne proizvodnje.

## 3.1. Pametni grad

S obzirom na stalan i ubrzan rast populacije u gradovima, učiniti održivima javne usluge zahtjeva traženje novih načina da bi se poboljšala iskoristivost javnih resursa, smanjene troškova i optimizacija glavnih infrastrukturnih komponenata grada. Tema nije nova, ali IoT može ponuditi razne načine koji bi ubrzali sveopći napredak. Koncept pametnog grada dobiva ogroman uspjeh koji se dalje nastavlja neometano dok ključnu ulogu u tome ima informacijsko-komunikacijska tehnologija - ICT (engl. *Information and Communication technology*). Takva vrsta tehnologije omogućuje veću uspješnost u kontekstu zaštite okoliša i potiče inovativnost u granama kao što su pametna opskrba vodom i energijom, inteligentni transportni sustavi (ITS) te upravljanje otpadom. Mobilna mreža pete generacije - 5G, će omogućiti temeljnu infrastrukturu za dizajn pametnog grada gdje se istodobno obrađuje velika količina podataka [6].

Tipične primjene za pametni grad obuhvaćaju široki spektar zadataka, od smanjenja troškova svakodnevnih usluga kao što su osvjetljenje ili upravljanje otpadom preko nadgledanja gradskih uvjeta kao što su kontrola buke, zagađenje zraka sve do poboljšanja dostupnih informacija o trenutnim prometnim zagušenjima i pitanju parkinga. Tablica 3. prikazuje usluge koje su obuhvaćene u kontekstu pametnoga grada [1].

**Tablica 3.** Usluge temeljene na IoT u okviru koncepta pametnoga grada

| Naziv usluge | Opis usluge |
|---|---|
| Pametno parkiranje | Nadzor popunjenosti parkirnih mjesta u gradu |
| Strukturalna ispravnost | Nadzor vibracija i stanja materijala građevinskih objekata, mostova, prometne infrastrukture i sl. |
| Mape gradske buke | Nadzor buke u stvarnom vremenu |
| Upravljanje prometnim zagušenjem | Praćenje vozila i pješaka u svrhu optimizacije rute vožnje ili pješačkih ruta |
| Pametna rasvjeta | Inteligentno i vremenu prilagodljivo upravljanje uličnom rasvjetom |
| Upravljanje otpadom | Detekcija popunjenosti kontejnera u svrhu optimiziranja rute odvoza |
| Inteligentni transportni sustavi | Pametne ceste i autoceste uz primjenu dinamičnih znakova upozorenja i diverzije u ovisnosti o vremenskim uvjetima i neočekivanim događajima poput nesreća ili zagušenja |

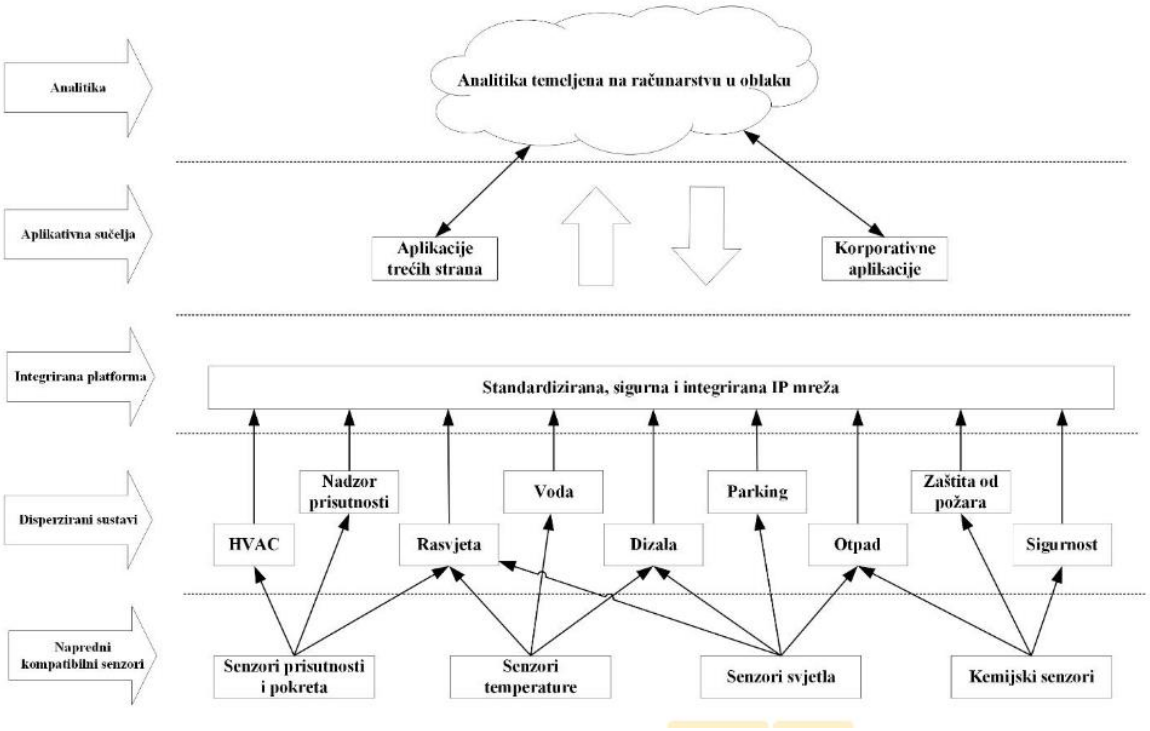
Izvor: [1].

Jedan od najvažnijih čimbenika pri ostvarenju cilja koji je u potpunosti pametni grad su prometne karakteristike. One mogu biti jako raznovrsne s obzirom na broj i vrstu usluga koje pružaju. Tipično urbano područje ima veliku gustoću i veliki broj prepreka za neke zahtjeve koje moraju biti uzete u obzir dok su s druge strane obujam prometa i kvaliteta usluge - QoS (engl. *Quality of service*) manje zahtjevni jer IoT urbane usluge nisu toliko kritične. Urbano područje obično ima dobru pokrivenost za sve vrste mreža pa tako dalekosežne i kratkosežne tehnologije odgovaraju tom području. Gledajući prometne karakteristike, širokopojasna mreža male snage - LPWAN (engl. *Low power wide area network*) može zadovoljiti kriterije i ponuditi lakšu implementaciju. S tehničkog stajališta, kreacija pametnog grada nije problem, dakle sve od prethodno navedenih usluga mogu biti lako razvijene i primijenjene koristeći trenutne tehnologije, ali glavno pitanje je pod kojom cijenom [5].

## 3.2. Pametne zgrade

Pametne zgrade za cilj imaju povećanje energetske efikasnosti i poboljšanje kvalitete života [4]. Zgrade čine oko 75% ukupne potrošnje električne energije na globalnoj razini, a procjenjuje se da je trećina te energije izgubljena [6].

Tipične aplikacije za pametne zgrade uključuju automatizirano osvjetljenje i kontrolu grijanja, praćenje potrošnje vode i energije, daljinsko upravljanje pametnim uređajima i prilagodbe prema željama korisnika i također otkrivanje anomalija radi povećane sigurnosti zgrade [5]. Vidljivi primjeri koji potvrđuju da okruženje pametne zgrade postoji duži niz godina su u programibilnom sustavu upravljanja grijanjem, hlađenjem i ventilacijom (engl. *Heating, Ventilation, Air-Condition,* HVAC) te u rasvjeti aktiviranoj pokretom. Primjena koncepta IoT kod pametne zgrade omogućuje upraviteljima veću kontrolu i učinkovitost upravljanja te bolju vidljivost komponenata zgrade. Slika 2. prikazuje arhitekturu okruženja pametne zgrade s primjenom koncepta IoT. Primjerice, kako bi se omogućilo autonomno prikupljanje relevantnih podataka, njihov prijenos, analiza i izvršavanje aktivnosti potrebna je, kako je vidljivo na slici, višestruka primjena raznovrsnih senzora u svrhu praćenja brojnih parametara poput: pokreta, osvjetljenja, tlaka zraka, temperature i protoka vode u različitim scenarijima. Vlasnicima pametnih zgrada omogućuje se jasnije upravljanje troškovima i resursima [1].




**Slika 2**. Arhitektura okruženja pametne zgrade s primjenom koncepta IoT, [1]

S gledišta podatkovnog prometa, pametne zgrade su relativno ne zahtjevne ali zahtijevaju skalabilnu infrastrukturu, zato jer je svaki objekt različit. Veličina mreže se obično sastoji od deset do sto povezanih uređaja. Obujam prometa je neregularan i povremen, zbog toga što se ljudi cijeli dan kreću zgradom. Međutim zahtjevi za QoS mogu biti visoki zato jer korisnici zahtijevaju manju latenciju kod korištenja uređaja.

Kratkosežne mrežne tehnologije bazirane na definiranom podatkovnom prometu pametnih zgrada bolje odgovaraju. Npr. WiFi je jako raširen i kako se pokazalo u mnogo slučajeva energetski resursi nisu najveći problem. Za ograničene uređaje, neki od WPAN (engl. *Wireless personal area network*) posebno dizajnirani za IoT (kao što su Bluetooth, ZigBee, Z-Wave, Thread, i dr.) mogli bi biti dobar izbor.

Pametne zgrade već imaju puno rješenja za primjenu i s obzirom na to da promet nije toliko zahtjevan sama tehnologija ne predstavlja veliki izazov. Puno veći problem predstavlja slaba interoperabilnost između uređaja koji su od različitih proizvođača i samim time ne koriste jednu zajedničku (istu) platformu kojom bi se moglo njima upravljati. Trenutno postoje dva pristupa rješavanju ovog problema. Prvi je predlaganje globalno prihvaćene mrežne tehnologije (npr. ZigBee, Z-Wave, Thread itd.) dok se drugi temelji na skrivanju temeljne mrežne tehnologije nudeći integracijski okvir [5].

## 3.3. Pametno zdravstvo

Pametno zdravstvo je domena o kojoj se dosta raspravlja u posljednje vrijeme i koja ima utjecaj na dvije grupe korisnika: pojedince i društvo. Pojedincima je glavni fokus na mogućnosti da prate svoje fizičke aktivnosti dok je cilj društva povećati kvalitetu medicinskih tretmana a smanjenje zdravstvenih troškova. Prednosti mogu biti ostvarene upotrebom nosivih uređaja koji imaju mogućnost praćenja zdravlja korisnika i prikazivanja trenutnih dijagnostičkih mogućnosti koje bi stvorile nove mogućnosti za liječenje raznih bolesti ili dobivanje ranih predviđanja za prevenciju istih. IoT može pomoći tako sto ima prave informacije u pravo vrijeme.

Primjena za pojedince se bazira na praćenju osobnog stanja koje uključuje mjerenje fizioloških promjena i analiza kretanja za klasifikaciju pojedinca. Ishod toga se može koristiti bilo gdje, od praćenja fizičke spreme do brige za djecu i starce. Slično tomu doktori i bolnice traže rješenja u skupljanju željenih informacija o zdravstvenom stanju pacijenata i pojednostavljenju evidencije i procesa distribucije podataka o pacijentima.

Prometne karakteristike prikazuju mogućnosti tih nosivih uređaja i zahtjeve za te zdravstvene aplikacije. Veličina mreže ovisi o aplikaciji. Koristeći nekoliko uređaja 'automatsko' praćenje može biti realizirano i u tom slučaju je veličina mreže mala dok praćenje pacijenata u bolnici zahtjeva srednju veličinu mreže sa stotinama uređaja koji pokrivaju čitavu zgradu. Zahtjevi za QoS su nesumnjivo visoki. Gubitak poruka ili duga kašnjenja su neprihvatljiva u hitnim slučajevima. Nosivi uređaji su na baterijski pogon i njihova trajnost je problem zbog visokog obujma prometa. Međutim mogu biti lako napunjeni. S obzirom na to da je veličina mreže mala do srednja, kratkosežne mrežne tehnologije su pravi izbor za ovaj sustav. Posebno RFID, Bluetooth i ZigBee koji su jako popularni u zdravstvenim aplikacijama jer koriste smartphone kao pristupnu točku.

Najveći izazov pri razvijanju rješenja za zdravstvo je kako zagarantirati kvalitetu i pristupačnost usluga a da istovremeno uređaji ostaju jednostavni, nosivi i da ne smetaju. Idealno bi bilo da osobe ili pacijenti koje pratimo ne moraju nositi nikakav uređaj i mogu biti praćeni s udaljenosti pomoću raznih senzora koji se nalaze oko njih [5].

## 3.4. Pametni okoliš

Pametni okoliš je nastojanje da se prati prostor oko nas za bolje razumijevanje tog prostora. Iako ne možemo kontrolirati sile prirode, pažljivim opažanjem možemo otkriti

različite prirodne pojave i reagirati na njih po potrebi. Posebno u slučaju rijetkih događanja kao što su prirodne katastrofe ključna je brza reakcija. IoT može ponuditi širok spektar mogućnosti za relativno male troškove koji mogu biti ekstremno povoljni u različitim scenarijima.

Kod praćenja prirodnog okoliša najveći fokus je na otkrivanju katastrofa kao što su šumski požari, potresi, tsunamiji, lavine, i dr. Međutim neka rješenja za cilj imaju pratiti manje kritične pojave kao što su zagađenje zraka ili praćenje divljih životinja. Veličina mreže može biti definirana kao srednja ili velika obično sa stotinama uređaja koji su povezani na jednom širokom području. S obzirom na to da je većina aplikacija bazirana na određivanju i praćenju rijetkih događaja, obujam prometa je neregularan i relativno rijedak. Iako s visokim zahtjevima za QoS. Aplikacije za pametni okoliš su tipično raspoređene u velikim ruralnim područjima tako da uređaji moraju biti pogonjeni baterijama. Iako bi punjene tih uređaja bilo ekonomski neizvedivo i zbog toga postoje pokušaji da se energetska potrošnja minimalizira ili da se iskoriste obnovljivi izvori energije. Kada pogledamo zahtjeve za pokrivenosti aplikacija za pametne okoliše to bi bila idealna domena za LPWAN [5].

## 3.5. Pametna energija

Područje pametne energije odnosi se na poboljšanja u distribuciji i potrošnji komunalnih usluga, poput električne energije, plina i vode. Proizvodnja električne energije je središnja točka budući da postoje globalni napori prema obnovljivim izvorima energije, koji proizvode ekološki prihvatljivu, ali fluktuirajuću energiju. Zbog svoje nestabilne prirode, električna mreža mora biti puno fleksibilnija i dinamičnija.

Aplikacije pametne energije precizno nadziru potrošnju energije i stvaraju obrasce koji se mogu koristiti za bolje razumijevanje korištenja energije. Međutim, sustav pametne mreže ne samo da poboljšava ravnotežu između proizvodnje i potrošnje energije, nego i podiže razumijevanje javnosti o učinkovitijoj uporabi energije. Veličina mreže je srednja do velika, osobito u velikim gradovima s mnogo kućanstava koji stvaraju veliku potražnju za učinkovitom uporabom mreže. Uređaji za pametnu energiju uglavnom su na mrežni pogon ili rjeđe na baterije. Pametna energetska domena zahtijeva dobru pokrivenost širokim područjem gdje prevladava LPWAN. Iako se prostorne mreže mogu temeljiti na tehnologijama kratkog dometa (npr. pametna brojila mogu se spojiti na kućni Wi-Fi), za prijenos i distribuciju energije potrebna je komunikacija na velikim udaljenostima.

Transformacija na održive i obnovljive izvore energije već je započela. U prošlom desetljeću razvijena su mnoga dobra rješenja, ali nestabilnost proizvodnje energije ostaje najveći tehnološki izazov koji zahtijeva značajne promjene u energetskoj mreži [5].

## 3.6. Pametni transport i mobilnost

Brza urbanizacija povezana s rastućim prometnim zagušenjima i globalizacijom tržišta stvorila je potražnju za upravljanje transportom i mobilnošću na pametniji način. Cilj je postići brži, jeftiniji i sigurniji prijevoz, što se može postići prikupljanjem svih vrsta podataka i njihovom analizom kako bi se pronašla optimalna rješenja [7].

Među aplikacijama pametne mreže i domene mobilnosti o kojima se najviše raspravlja, nesumnjivo su automatizirana i autonomna vozila, jer je povezana svakoj korisničkoj skupini: pojedincima, društvu, kao i industriji. Ipak, druge tipične primjene uključuju lokalizaciju i praćenje vozila, kvalitetu praćenja pošiljke, dinamičko upravljanje semaforima na temelju trenutne prometne situacije i praćenje stanja cesta. Područje pametnog transporta i mobilnosti može biti zahtjevno u smislu prometnih karakteristika. Broj senzora u vozilima rapidno raste dok brzina prometa varira ovisno o usluzi. Zahtjevi za QoS obično su visoki. Uređaji za pametni transport i mobilnost uglavnom se napajaju baterijama u vozilu ili mrežnim napajanjem za uređaje uz cestu, pa preciznost i točnost imaju prednost nad uštedom energije.

Definitivno, komunikacija između vozila mora se graditi na tehnologijama kratkog dometa, dok lokalizacija i nadzor vozila zahtijevaju dugosežnu mrežnu tehnologiju. Stoga je potrebno pogledati svaku uslugu pojedinačno [5].

## 3.7. Pametna proizvodnja

Globalizacija i povećanje očekivanja potpuno prilagodljivih proizvoda stvaraju visoke zahtjeve za proizvodnju i maloprodaju. Kako bi se pratio ovaj trend, proizvodnja mora ponuditi kraća razdoblja razvoja, veliku količinu fleksibilnosti, učinkovitost resursa i nove inovativne modele poslovanja. IoT može pružiti informacije u stvarnom vremenu zbog masovne primjene kiber-fizičkih sustava, što je također uzrok sljedeće industrijske revolucije, nazvane Industrija 4.0.

U ovom području, cilj je poboljšati proizvodnu liniju primjenom osiguranja kvalitete i fleksibilnog prilagođavanja, praćenjem zaliha za učinkovitije upravljanje lancem opskrbe, koristeći lokalizaciju predmeta i radnika, praćenje okoliša kako bi se osigurali sigurni uvjeti,

kao i praćenje strojeva radi optimizacije njihovih rasporeda održavanja i popravaka. Veličina mreže pametne proizvodnje i maloprodaje obično je srednja do velika, s obzirom na količinu predmeta, strojeva i radnika koje treba nadzirati. Obujam prometa je i pravilan i nepravilan jer više aplikacija prikuplja podatke o izvješćima o uvjetima proizvodnje. Uređaji za pametnu proizvodnju i maloprodajno područje pokrivaju veliki broj zadataka i s obzirom na iskorištenost mogu biti pasivni, na električnu mrežu (napajanje) ili na baterije.

Budući da se većina proizvodnih i maloprodajnih procesa odvija u zatvorenom, mrežne tehnologije kratkog dometa igraju važnu ulogu. Konkretno, RFID je vrlo popularna tehnologija kratkog dometa zbog dostupnosti pasivne i jeftine RFID oznake. Bez obzira na to, također tehnologije mreža velikog dometa nalaze svoju primjenu u proizvodnji [5].

# 4. Bežične komunikacijske tehnologije korištene u konceptu IoT

Bežični način povezivanja se pokazao najpraktičnijim i najboljim za povezivanje pojedinih dijelova IoT sustava na Internet. S time, jedan od sastavnih dijelova Internet stvari jest bežična senzorska mreža - WSN (engl. *Wireless Sensor Network*) ili bežična senzorska i aktuatorska mreža - WSAN (engl. *Wireless Sensor and Actuator Network*). Oni se sastoje od senzora i/ili aktuatora koji se još i nazivaju čvorovi te služe za prikupljanje podataka iz okoline, a u određenim slučajevima služe i za izvršavanje i kontrolu zadataka. Internet kakav mi poznajemo baziran je na internetskom protokolu koji je održavan od strane skupine za internetsko inženjerstvo - IETF (engl. *Internet Engineering Task Force*), a korištenje IP adresa kako bi se identificirali povezani uređaji i preusmjeravali podaci s vremenom su postali svakodnevica. Istovremeno, brojni bežični komunikacijski uređaji i tehnologije su razvijeni kako bi zadovoljili potrebe IoT aplikacija, no to je dovelo do određenih problema u kompatibilnosti [5].

U nastavku su prikazani neki od protokola koji su nastali razvojem bežičnih komunikacijskih tehnologija, a međusobno su podijeljeni na mreže kratkog i dugog dometa.

## 4.1. Mreže kratkog dometa

Mreže kratkog dometa koriste bežičnu tehnologiju koja komunicira u dometu od nekoliko centimetara pa do nekoliko stotina metara. Neki od njih su [5]:

- RFID,
- NFC,
- BLE - Bluetooth s niskom potrošnjom energije (engl. *Bluetooth Low Energy*),
- Ant,
- EnOcean,
- Z-Wave,
- Insteon,
- Zigbee,
- MiWi,
- DigiMesh,
- WirelessHART,
- Thread,
- 6LowPAN - široko područje mreže male snage (engl. *Low power wide area network*) i
- Wi-Fi.

U nastavku će biti ukratko objašnjene neke od navedenih bežičnih komunikacijskih tehnologija.

**RFID** koristi elektromagnetska polja kako bi automatski identificirala i pratila oznake označene na objektima. Takav sustav sastoji se od malog radio transpondera i radio primopredajnika. U trenutku poklapanja elektromagnetskog impulsa od strane RFID čitača u blizini, oznaka odašilje digitalni podatak. Takav podatak uglavnom predstavlja identifikacijsku oznaku. S time, ovakav sustav idealan je za korištenje prilikom obavljanja inventure [8].

**Z-Wave** je bežični komunikacijski protokol primarno korišten za osobnu upotrebu. Koristi nisko-energetske radio valove i komunicira od uređaja do uređaja. Takav način omogućuje bežičnu kontrolu stambenih uređaja i drugih, kao sto su kontrola osvjetljenja, sigurnosnih sustava, termostata, prozora itd. [19]. Z-Wave pokriva otprilike 30m point-to-point komunikacije i specijaliziran je za uređaje kojima je potreban mali prijenos podataka [9].

**Zigbee** je bežična tehnologija razvijena kao otvoreni globalni standard kako bi adresirala specifične potrebe jeftinih bežičnih IoT mreža male snage. takav standard definiran je IEEE 802.15.4 fizičkim radio specifikacijama i djeluje na nelicenciranim frekvencijskim pojasevima uključujući 2.4 GHz, 900 MHz i 868 MHz [10].

**Wi-Fi** je bežična mrežna tehnologija koja dozvoljava uređajima poput računalima, mobitelima i ostalima spajanje na Internet. Svima umreženim uređajima dozvoljava međusobnu razmjenu informacija stvarajući mrežu. Spajanje na Internet omogućeno je bežičnim ruterom [11].

## 4.2. Mreže dugog dometa

Mreže dugog dometa koriste bežičnu tehnologiju koja komunicira u dometu od nekoliko desetaka kilometara, kako bi pokrili velike površine. Neki od njih su [5]:

- LoRaWAN - široko područje mreže male snage (engl. *Low power wide area network*),
- Symphony Link,
- Weightless,
- SIGFOX,
- DASH7,
- eMTC - poboljšana komunikacija o vrsti stroja (engl. *enhanced Machine Type Communication*),
- NB-IoT - uskopojasni internet svari (engl. *NarrowBand Internet of Things*,) i

- EC-GSM-IoT - prošireno pokrivanje GSM Internet stvari (engl. Ex*tended Coverage GSM IoT*).

U nastavku slijedi kratko objašnjenje nekih od spomenutih tehnologija dugog dometa.

**LoRaWAN** definirana je malom potrošnjom i širokom površinom mreže. to je protokol dizajniran za bežično povezivanje uređaja na internet na različitim razinama (regionalnoj, nacionalnoj i globalnoj razini). Ciljna platforma je Internet stvari zato sto omogućuje dvosmjernu komunikaciju, *end-to-end* sigurnost, mobilnost i lokalizaciju [12].

**SIGFOX** radi na principu diferencijskog binarnog faznog pomaka (engl. *Differential binary phase-shift keying*, DBPSK) i gausovog frekvencijskog pomaka (engl. *Gaussian frequency shift keying*, GFSK) i time omogućuje komunikaciju pomoću industrijskog, znanstvenog i medicinskog radio pojasa. Signal još može biti korišten kako bi pokrio velike površine te pristupio objektima ispod zemlje [13].

**eMTC** je tehnologija male snage i široke pokrivenosti koja podržava IoT kroz manju kompleksnost uređaja i pruža proširenu pokrivenost mobilnih nosioca postojećih LTE baznih stanica. eMTC je poznat po visoko podatkovnoj usluzi kod značajnijih IoT aplikacija [14].

**NB-IoT** je standardizirana tehnologija bazirana na maloj potrošnji i širokoj pokrivenosti. Razvijena je kako bi se proširio krug IoT uređaja i usluga. Ovakva tehnologija poboljšava potrošnju korištenih uređaja, sistemski kapacitet i spektar efikasnosti, pogotovo u dubokoj pokrivenosti. Novi fizički sloj dizajniran je za stvaranje signala i kanala kako bi se uskladili potrebni zahtjevi proširene pokrivenosti (izvangradska ili seoska područja) [15].

## 4.3. Usporedba tehnologija

U tablici 4. prikazana je usporedba spomenutih komunikacijskih tehnologija, te njihove razlike u frekvenciji, dometu, brzini prijenosa, vrsti topologije koju koriste i energetske učinkovitosti. Primjerice, u tablici se vidi da se tehnologija Wi-Fi koristi za kraće udaljenosti međutim ima veliku brzinu prijenosa, dok za razliku, tehnologija LoRaWAN koristi veće udaljenosti ali zato ima značajno manju brzinu prijenosa. Dok s aspekta energetske učinkovitosti, LoRaWAN ima puno veći vijek trajanja baterije. Wi-Fi je vrlo zahtjevna tehnologija, koja troši puno energije u usporedbi sa ostalim bežičnim tehnologijama i zato se ne koristi za uređaje koji rade na bateriju.

Za odabir komunikacijske tehnologije ovisit će mnogi parametri poput područja primjene koncepta IoT i specifičnosti pojedine usluge za različite zahtjeve [1].

**Tablica 4.** Usporedba tehnologija.

| Tehnologija | Frekvencija | Domet | Brzina | Topologija | Trajanje baterije uređaja |
|---|---|---|---|---|---|
| **RFID** | niska / visoka / ultravisoka | 1 cm – 100 m | 1 – 100 kbps | peer-to-peer | N/A (pasivni način rada) / 3-5 godina (aktivni način rada) |
| **Z-Wave** | do 1 GHz | 40 – 200 m | 100 kbps | mesh | Nekoliko mjeseci - nekoliko godina |
| **Zigbee** | do 1 GHz, 2.4 GHz | 10 – 100 m | 250 kbps | zvijezda / mesh / tree | Nekoliko mjeseci - nekoliko godina |
| **Wi-Fi** | 2.4 GHz, 5 GHz | 100 m | od Mbps do Gbps | zvijezda | Nekoliko dana - nekoliko godina |
| **LoRaWAN** | do 1 GHz | 10 – 15 km | 50 kbps | zvijezda | 10 + godina |
| **SIGFOX** | do 1 GHz | 10 – 50 km | 100 bps | zvijezda | 10 + godina |
| **eMTC** | 450 MHz – 3.5 GHz | 10 – 15 km | 1 Mbps | zvijezda | 10 + godina |
| **NB-IoT** | 450 MHz – 3.5 GHz | 10 – 15 km | 250 kbps | zvijezda | 10 + godina |

Izvor: [5]

## 4.4. Zajednički protokoli

Brojni IoT standardi su predstavljeni kako bi olakšali i pojednostavnili poslove programera i pružatelja usluga. U nastavku će biti predstavljene četiri kategorije u kojima su podijeljeni protokoli, a to su [2]:

- Aplikacijski protokoli (engl. *Application Protocols*),
- Protokoli za otkrivanje usluge (engl. *Service Discovery Protocols*),
- Infrastrukturni protokoli (engl. *Infrastructure Protocols*) i
- Ostali utjecajni protokoli (engl. *Other Influential Protocols*).

U tablici 5. prikazane su četiri kategorije spomenutih protokola.

**Tablica 5.** Prikaz protokola

| | | | | | | |
|---|---|---|---|---|---|---|
| **Aplikacijski protokoli** | CoAP | MQTT | XMPP | AMQP | DDS | |
| **Protokoli za otkrivanje usluge** | mDNS | DNS-SD | | | | |
| **Infrastrukturni protokoli** | RPL | 6LowPAN | IEEE 802.15.4 | BLE | EPCglobal | LTE-A |
| **Ostali utjecajni protokoli** | IEEE 1888.3, IPSec | IEEE 1905.1 | | | | |

Izvor: [2]

### 4.4.1. Aplikacijski protokoli

Svrha i cilj protokola koje koristi IoT je osiguranje korisne informacije kroz obradu i upravljanje velikom količinom podataka i informacija. Na taj način koncept internet stvari omogućuje poboljšanje kvalitete života jer osigurava umrežavanje različitih stvari i objekata putem interneta, bez ljudskog sudjelovanja. Aplikacijski protokoli su najbrojniji po broju implementacija [16].

Aplikacijski protokoli se sastoje od protokola [2]:

- Ograničen aplikacijski protokol (engl. *Constrained Application Protocol*, CoAP),
- Prijenos telemetrije reda čekanja poruka (engl. *Message queue telemetry transport*, MQTT),
- Proširivi protokol za razmjenu poruka i prisutnost (engl. *Extensible Messaging and Presence Protocol*, XMPP),
- Napredni protokol za čekanje poruka (engl. *Advanced Message Queuing Protocol*, AMQP) i
- Usluga distribucije podataka (engl. *Dana Distribution Service*, DDS).

CoAP je specijalizirani mrežni transferni protokol za korištenje s ograničenim uređajima i mrežama u IoT. Dizajniran je kako bi omogućio jednostavnim ograničenim uređajima umrežavanje u IoT sustav, čak i kroz ograničene mreže s uskim frekvencijskim pojasom i niskom dostupnosti. CoAP se bazira na reprezentativnom statusnom prijenosu - REST-u (engl. *Representational State Transfer*,), a to je jednostavniji način za razmjenu podataka između klijenta i servera preko HTTP-a (engl. *Hypertext transfer protocol*) [2,17].

MQTT je protokol za poruke za ograničene mreže (mreže sa slabim frekvencijskim pojasom) i IoT uređaje s ekstremno visokom latencijom. Bas zato što je takav protokol specijaliziran za nisko-pojasna okruženja, kao i ona s visokom latencijom, idealan je protokol

za M2M komunikaciju. MQTT služi za povezivanje pojedinih dijelova u sustav oblaka (engl. *cloud*). Stvoren je na vrhu protokola upravljanja prijenosom - TCP (engl. *Transmission Control Protocol*), a jednostavno se sastoji od 3 glavne komponente, a to su pretplatnik (engl. *subscriber*), izdavač (engl. *publisher*) i posrednik (engl. *broker*) [2,18].

XMPP je otvoreni komunikacijski protokol dizajniran za trenutačno posredovanje poruka, informacije o prisutnosti i održavanje liste kontakta. Baziran je na XML (engl. *Extensible Markup Language*), omogućuje razmjenu strukturiranih podataka između dvaju ili vise mrežnih entiteta u približno stvarnom vremenu. Korištenje za razmjenu poruka između vise korisnika, zvučni i video pozivi, također XMPP dozvoljava korisnicima međusobnu komunikaciju slanjem trenutnih poruka na Internet bez obzira koji operacijski sustav koriste [2,19].

AMQP je protokol za otvoreni standardni aplikacijski sloj za softvere usredotočene na razmjenu poruka. Definiraju ga orijentiranost prema porukama, njihovo uvođenje u red i usmjeravanje uključujući *point-to-point* i *publish-and-subscribe* protokole, također pouzdanost i sigurnost [20].

DDS za sustave u stvarnom vremenu je objektna kontrolna grupa (engl. *Omg object management group*) za m2m standard koji omogućuje pouzdane, interoperabilne , skalabilne razmjene podataka visokih performansi u stvarnom vremenu koristeći *publish–subscribe* uzorak [21].

### 4.4.2. Protokoli za otkrivanje usluge

Protokoli ove kategorije mogu otkriti resurse i usluge koje nude IoT uređaji. Dva najdominantnija protokola u ovoj kategoriji su [2]:

- Multicast DNS (mDNS) i
- DNS Service Discovery (DNS-SD).

mDNS protokol kod računalnog umrežavanja dodjeljuje IP adresu svakom terminalnom uređaju unutar manjih mreža koje ne uključuju lokalno ime servera. Pripada usluzi nulte konfiguracije koristeći jednaka programska sučelja, formate paketa i operacijsku semantiku kao DNS (engl. *Domain Name System*) [22]. Za razliku od DNS-a, mDNS je fleksibilan zbog toga što imenski prostor kod DNS-a je korišten lokalno bez dodatnih potrošnji i konfiguracija [2].

DNS-SD standard omogućuje klijentima otkrivanje svih mogućih imenovanih instanci određene usluge, tako sto daje određeni tip usluge koju klijent traži i domenu u kojoj klijent traži navedenu uslugu [23]. takav standard koristi mDNS kako bi poslao DNS pakete specifičnim adresama preko UDP-a (engl. *User Datagram Protocol*). Postoje dva glavna koraka u takvom procesu otkrivanja usluga: pronalazak imena terminalnih uređaja potrebnih usluga kao sto su printeri ili IP adrese za uparivanje s njihovim terminalnim uređajima pomoću mDNS-a [2].

### 4.4.3. Infrastrukturni protokoli

Infrastrukturni protokoli su potrebni za uspostavu temeljne komunikacije potrebne IoT aplikacijama. Neki od često korištenih infrastrukturnih protokola su [2]:

- Routing Protocol for Low Power and Lossy Networks (RPL),
- 6LowPAN,
- IEEE 802.15.4,
- BLE,
- EPCglobal i
- LTE-A.

U nastavku će biti objašnjeni navedeni infrastrukturni protokoli.

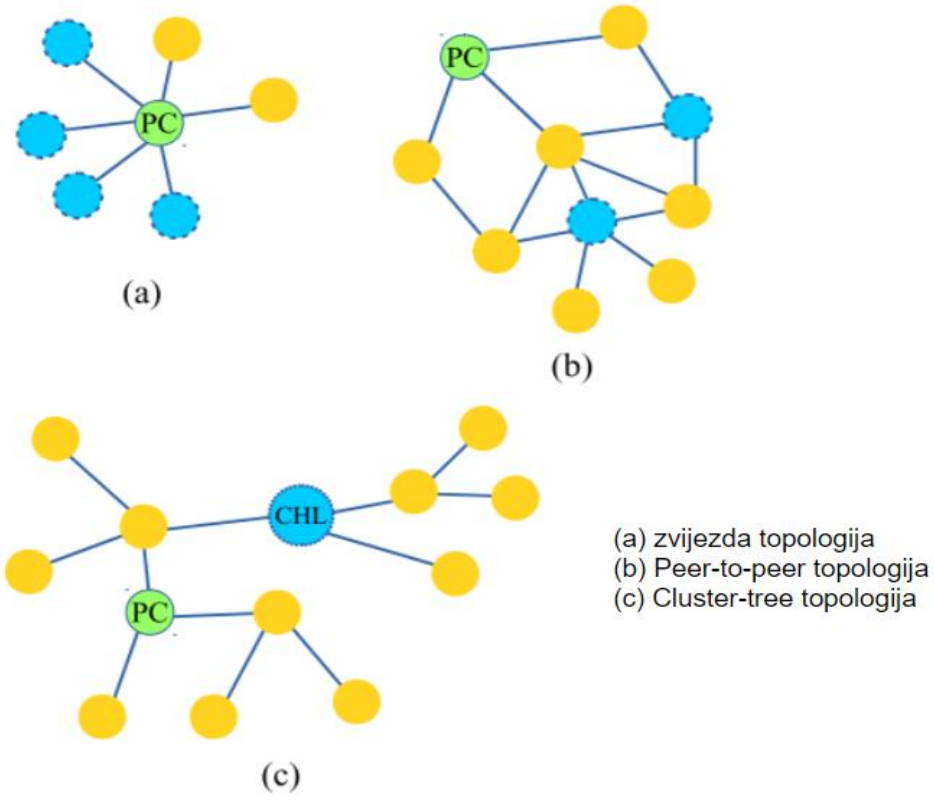
RLP jest protokol za preusmjeravanje kod bežičnih mreža s malom potrošnjom i generalno osjetljiv za gubitak paketa. To je proaktivan protokol temeljen na udaljenim vektorima i funkcionira u skladu s IEEE 802.15 standardom [24]. kako bi se očuvale topologija i informacije za preusmjeravanje, RPL koristi četiri tipa kontrolnih poruka. Medu njima najbitnija je poruka usmjereni aciklički graf usmjeren na odredište - DODAG (engl. *Destination Oriented Directed Acyclic Graph*) informacijski objekt koji služi kako bi se sačuvao trenutni nivo čvora [2].

6LowPAN je koncept koji je nastao iz ideje da internetski protokol treba i može biti korišten i kod najmanjih uređaja, stoga uređaji s malom potrošnjom i ograničenim procesnim mogućnostima trebaju imati mogućnost pristupa internetu stvari [25]. za razliku od navedenih protokola ovaj se razlikuje u određenim dijelovima kao sto su: ograničena veličina paketa, varirajuća duljina adrese i uski frekvencijski pojas [2].

IEEE 802.15.4 jest standard koji definira bežična osobna područja mreža nižih stopa (engl. *Low-rate wireless personal area networks*, LR-WPANs). Definira fizički sloj kao i

kontrolu medijskog pristupa za LR-WPANs te je reguliran od strane IEEE 802.15 standarda. Ovaj standard je baza za Zigbee, WirelessHART, MiWi, 6LoWPAN i Thread komunikacijske tehnologije, a svaka od njih sadrži određena proširenja koja nisu sastavni dio IEEE 802.15.4 standarda [26].

Standardne topologije koje formiraju IEEE 802.15.4 mreže su: zvijezda (engl. *Star*), *peer-to-peer* i *cluster-tree*, kako je prikazano na slici 3.




**Slika 3.** Primjer topologije standarda IEEE 802.15.4

Izvor:[2]

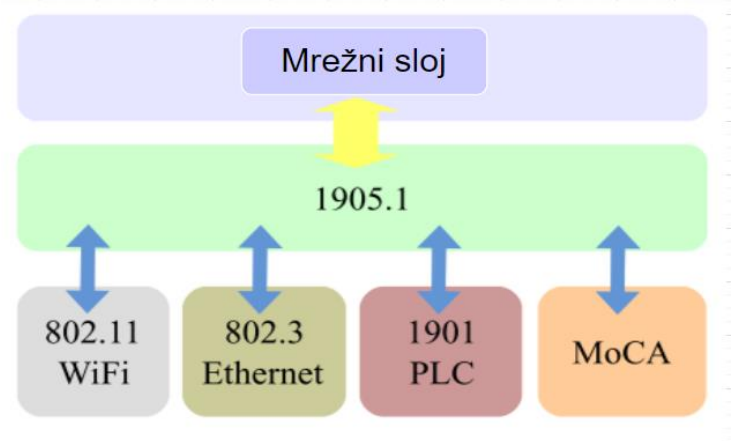
BLE je bežična osobna mrežna tehnologija dizajnirana i dovedena na tržište od strane Bluetooth SIG - bluetooth specijalne interesne grupe (engl. *Bluetooth Special Interest Group*). Njen primarni cilj je implementacija u novijim uređajima  koji bi se koristili u zdravstvene, sportske, sigurnosne i rekreativne svrhe [27]. Ova inačica bluetooth-a koristi kratko dometni radio signal s minimalnom potrošnjom kako bi radila duži vremenski period (i do nekoliko godina) za razliku od svojih prijašnjih verzija [2].

EPCglobal je GS1 inicijativa za inovaciju i razvoj industrijskih standarda za elektronički proizvodni program - EPC (engl. *Electronic Product Code*), kako bi se podržalo korištenje RFID-a i globalna vidljivost u sadašnjim rastućim informacijskim sadržajima [28]. Ovakva arhitektura obećava reorganiziranu tehnologiju za budućnost IoT, zbog njene otvorenosti, skalabilnosti, interoperabilnosti i pouzdanosti [2].

LTE-A je standard mobilnih umrežavanja koji omogućuje bolje performanse od svoje starije verzije LTE standarda. Ovaj standard omogućuje prijenos čak i do jedan gigabajt podataka u sekundi, zahtjeva širi frekvencijski pojas te koristi mimo (engl. *Multiple-input, multiple-output*) tehnološki pristup [29]. Arhitektura LTE-A mreža zasnovana je na dvama ključnim dijelima. Prvi dio je bazna mreža (engl. *Core network*, CN) te ona kontrolira mobilne uređaje i njihove IP adrese. Drugi dio pripada radio pristupnoj mreži - RAN-u (engl. *Radio Access Network*), koji omogućuje bežičnu komunikaciju i radijski pristup i ustaljuje korisničke protokole [2].

### 4.4.4. Ostali utjecajni protokoli

Što se tiče ostalih protokola, od važnosti su sigurnost i interoperabilnost (IEEE 1905.1). Nova obilježja i mehanizmi interneta stvari ne mogu biti osigurani konvencionalnim sigurnosnim protokolima koji su korišteni na internetu. Sigurnosni protokoli na internetu dizajnirani su kako bi radili na uređajima poput stolnih i prijenosnih računala. Dalje, IEEE 802.15.4 sigurnosni protokol omogućuje mehanizme za komunikacijsku zaštitu između dva susjedna uređaja [2].




**Slika 4**. IEEE 1905.1 funkcionalnost

Izvor: [2]

Raznolikost uređaja unutar okoline IoT oslanja se na različite mrežne tehnologije, stoga je potrebna interoperabilnost korištenih tehnologija. IEEE 1905.1, čije su funkcionalnosti prikazane slikom 4., standard dizajniran je kako bi se konvergirale kućne mreže i heterogene tehnologije. Omogućuje apstraktni sloj koji skriva raznolikost pristupa medijskoj kontroli , dok s druge strane ne zahtijeva promjene u uređajima kao samima [2].

# 5. Sigurnost bežičnih komunikacijskih tehnologija

Živjeti u 'pametnom' gradu podrazumijeva konstantno širenje i rast mreže međusobno povezanih uređaja koji služe prikupljanju i razmjeni podataka. Zahvaljujući internetu stvari, pametni uređaji poput termostata, rasvjete i drugih senzora, omogućena je značajna mogućnost za buduća poslovanja i proizvođače. U svakom sustavu neophodno je uvesti određenu dozu sigurnosti, stoga je i u ovom području predstavljen izraz sigurnost u internetu stvari. To je tehnološko područje koje se bavi sigurnosnim protokolima povezanih uređaja i mreža unutar IoT. Internet stvari omogućuje povezivanje na internet jednom takvom sustavu koji se može sastojati od računalnih i mehaničkih uređaja, objekata, životinja pa i ljudi. Sigurnost IoT postala je jedna od bitnih tema rasprave nakon sto je došlo do određenog broja incidenata uobičajenih IoT uređaja koji su do tada bili korišteni. Dakle, sigurnosne mjere su kritične za mreže te uređaje spojene na njih. Ključni sigurnosni problemi unutar IoT sustava sastoje se od zaštite dviju kritičnih točaka, a to su povjerljivi podaci i provjera identiteta. Dalje, postoji još pet glavnih zahtjeva u informacijskoj sigurnosti, a to su: dostupnost podataka, povjerljivost podataka, integritet podataka, autentičnost i autorizacija [30, 31].

Dostupnost podataka je ključno u IoT. Ono doprinosi pristupu sigurnosti i pouzdanosti dostupnih podataka. IoT sustav mora omogućiti sigurnosnu kopiju bitnih informacija kako bi se spriječio gubitak podataka [32].

Povjerljivost podataka zahtjeva zaštitu podataka koristeći određene enkripcijske tehnike i mehanizme kako bi se spriječilo razotkrivanje podataka kao i bilo kakav neovlašten pristup IoT opremi i uređajima [32].

Integritet podataka se poziva na zaštitu vrijednih i osjetljivih informacija od hakerskih napada. Određeni događaji utječu na integritet podataka, kao na primjer zastoj servera [32].

Autentičnost i autorizacija također igraju važnu ulogu u sigurnosti Internet stvari. Oni provjeravaju identitet korisnika ili uređaja i tako pružaju pristup ostalim bezopasnim uređajima i uslugama [32].

Osnovna načela sigurnosti (povjerljivost, cjelovitost i dostupnost) ili CIA (engl. *Confidentiality, Integrity and Availability*) nisu dovoljna pri uvažavanju novih prijetnji koje se javljaju kao rezultat primjene koncepta internet stvari. Stoga se uz CIA trijadu, predlažu dodatna sigurnosna načela: neporecivost, privatnost, revizija, odgovornost i vjerodostojnost, kako je prikazano tablicom 6 [1].

**Tablica 6.** Proširena načela sigurnosti u okruženjima primjene koncepta IoT, [1]

| Načelo sigurnosti | Obrazloženje | Resursi IK sustava na koje se načelo odnosi | | | | | |
|---|---|---|---|---|---|---|---|
| | | Podatci | Korisnici | Procesi | Hardver | Softver | Mreža |
| **Povjerljivost** | Isključivo autorizirani korisnici/procesi imaju pravo uvida i pristupa resursima IK sustava | | • | | | | |
| **Cjelovitost** | Isključivo autorizirani korisnici imaju pravo izmjene podataka u IK sustavu | | | • | | | |
| **Dostupnost** | IK resursi moraju biti dostupni legitimnom korisniku/procesu u traženo vrijeme i prema zadanim uvjetima | • | • | • | • | • | • |
| **Neporecivost** | Sudionici transakcije koja se odvija posredstvom IK sustava ne mogu poreći provedbu transakcije | • | • | • | • | • | • |
| **Privatnost** | Sposobnost IK sustava da provodi definirana pravila privatnosti omogućavajući korisniku kontrolu nad osjetljivim podatcima | • | | | | | |
| **Revizija** | Sposobnost IK sustava da omogući provedbu revizije aktivnosti u slučaju nepoželjnog događaja | • | • | • | • | • | • |
| **Odgovornost** | Sposobnost IK sustava da nametne odgovornost korisniku za poduzete aktivnosti | • | | • | | | |
| **Vjerodostojnost** | Sposobnost IK sustava da jednoznačno utvrdi identitet i osigura povjerenje između trećih strana (korisnika/procesa) | • | • | | | | |

Sigurnosne metode IoT ovise o specifičnoj aplikaciji ili ekosustavu koji IoT obuhvaća. Od strane proizvođača IoT uređaja, oni trebaju omogućiti siguran hardver, osigurati sigurnosna ažuriranja kao i dinamička testiranja. S druge strane, razvojni inženjeri bi se trebali fokusirati na sigurnost razvoja softvera i sigurnu integraciju korištenih IoT uređaja [32].

Za potpunu zaštitu, svaka podatkovna točka mora biti zaštićena određenom metodom enkripcije od trenutka njenog stvaranja pa do konačnog IoT uređaja. Enkripcija štiti i izolira podatke između korisnika, kompanija i trećih strana koji imaju pristup podacima. Ona također daje određenu dozu sigurnosti organizacijama koje razmjenjuju osjetljive informacije sa svojim korisnicima [33].

Na slici 5. prikazana povećana potražnja za enkripcijom podataka u proteklih nekoliko godina, s lijeve strane na cloud platformi te s desne strane na IoT platformi.


**Slika 5.** Enkripcija podataka

Izvor: [34].

# 6. Izazovi komunikacije u konceptu IoT

Internet stvari je tema oko koje se dosta raspravlja u zadnje vrijeme, poglavito zbog potencijala koje može pružiti te stoga privlači velik interes od strane industrijskog i akademskog razvoja. Doduše, još uvijek je daleko od svakodnevne uporabe, stoga su brojni istraživači uključeni u razvoj kako bi se to postiglo [5].

Jedan od glavnih izazova kako je spomenuto u prethodnom poglavlju bit će sigurnost. Sigurnost pogotovo može biti narušena gdje god su uređaji povezani u mreže velikih razmjera. Komponente internet stvari poput RFID, WSN, pa i oblak posebno su osjetljivi na hakerske napade u kojima je cilj onesposobiti mrežu, dostaviti u nju pogrešne podatke ili pristupiti osjetljivim podacima. Od nabrojanih komponenti, RFID prema svom načinu rada može biti posebno ranjiv jer je njegova glavna funkcionalnost praćenje objekata ili ljudi. Ovakav problem bi se mogao riješiti enkripcijom jer ona osigurava autentičnost podataka koji i kad bi 'procurili' nekim trećim stranama ne bi bili iskoristivi. Naravno ista metoda zaštite ne može djelovati vječno pa je veoma bitno dovoljno često ažurirati nove načine zaštite. Enkripcija veoma uspješno štiti od napadača izvana, no s druge strane ne štiti od unutarnjih napada. S vremena na vrijeme potrebno je reprogramirati čvorove u mreži. Reprogramiranje omogućuje provjeru ispravnosti novonastalih programa te obustavlja bilo kakve zlonamjerne instalacije.

Zaštita oblaka također predstavlja izazov u budućnosti, pogotovo u slučajevima hibridnih oblaka gdje se koriste privatni i javni dijelovi. Također, spremanje podataka u oblak ima pozitivne i negativne strane bez obzira na moguće napade. S jedne strane, pozitivni aspekt prikupljanja podataka je personalizirano oglašavanje, dok s druge strane negativni aspekt prikupljanja podataka može biti nenamjerno korištenje osobnih podataka u javnosti [35].

Još neki od izazova su skalabilnost, samoorganizacija i energetska učinkovitost. S obzirom na golem broj uređaja koji zahtijevaju istodobno povezivanje, skalabilnost u IoT sustavima postala je zabrinjavajuća. Postoje uglavnom dvije vrste problema skalabilnosti, a to su vertikalna i horizontalna skalabilnost. Skalabilnost se odnosi na dodavanje ili uklanjanje računalnih resursa IoT čvora, odnosno dodavanje ili uklanjanje IoT čvora. S obzirom na svoju važnost, skalabilnost internet stvari opsežno se obrađuje u literaturi s prijedlogom računalstva u oblaku, ali unatoč tim naporima izazovi i dalje ostaju, poput IoT čvorova koji

trebaju pružiti povećani broj usluga, kao što su funkcionalna skalabilnost, kontrola pristupa, pohrana podataka, tolerancija grešaka te privatnost i sigurnost.

U tijeku je promjena paradigme s interneta stvari na interneta svega (engl. *Internet of Everything,* IoE) zbog širenja IoT čvorova, što zahtijeva nove pristupe autonomnom upravljanju kako bi mreža postala proaktivna, a ne reaktivna. Glavna ideja samoorganizacije u IoT sustavima je aktivno reagiranje na promjenjiva okruženja na automatski i koordiniran način. U ovom području postoji mnogo otvorenih izazova, a neki značajni pravci istraživanja u budućnosti uključuju bavljenje heterogenom interoperabilnošću sustava, projektiranje optimalnih samoorganizacijskih protokola i dr. [36].

IoT stvara milijarde uređaja i mreža s velikom raznolikošću spojenom na internet. Energija se smatra aktualnim resursom za IoT pametne uređaje jer se većina aplikacija napaja iz baterije ili koristi tehnike prikupljanja energije. To znači da nije pametno gubiti energiju prijenosom nepotrebnih podataka i protokolarnih opterećenja u odnosu na postojeće protokole poput HTTP-a, TCP-a itd. Stoga je projektiranje energetski učinkovite mrežne arhitekture i mehanizma inteligentnog usmjeravanja i dalje veliki izazov u IoT mrežama [37].

# 7. Zaključak

Internet stvari zadnjih godina postaje sve aktualnija tema, a ubrzan rast uređaja približava ideju koncepta internet svari. Funkcije takvog koncepta potrebno je uklopiti u svakodnevnu pozadinu kako bi nove mogućnosti mogle biti ostvarene.

Pogledom na arhitekturu može se primijetiti kako bi IoT trebao biti sposoban povezati velik broj heterogenih objekata putem interneta, te su u tu svrhu predstavljeni određeni modeli arhitekture. Dalje, idealni IoT sustav sastoji se od glavnih elemenata koji su: identifikacija, senzoriranje, komunikacija, procesiranje, usluge i semantika. Optimalnim iskorištavanjem arhitekture i datih elemenata mogu se izvesti razna područja primjene, od pametnih gradova, okoliša, zdravstva itd. Usprkos velikim načinima povezivanja, bežični se pokazao najpraktičnijim za povezivanje pojedinih dijelova IoT sustava na internet, sukladno s time razvijeni su brojni protokoli a svaki od njih ima svoje prednosti i nedostatke.

Ključni dio koncepta internet stvari je M2M, odnosno direktna komunikacija između uređaja koji koriste žične ili bežične komunikacijske kanale. Iz dana u dan broj uređaja povezanih na internet raste ekstremno brzo. Zahvaljujući tome, primjene koncepta internet stvari poput 'pametnog' grada su uvelike olakšale svakodnevni život. Npr. 'pametan' parking olakšava vozaču potragu za parkingom jer je broj i pozicija slobodnih mjesta vidljiva na aplikaciji. Otežavajuće okolnosti u primjeni 'pametnog' grada i u ostalim područjima primjene koncepta IoT jesu značajna financijska ulaganja u infrastrukturu. Zato u svakodnevnom životu svjedočimo rijetkim primjenama 'pametnog' grada kao i u većini ostalih područja primjene.

Ne smije se zaboraviti na određenu dozu sigurnosti, koja također predstavlja jedno tehnološko područje, a bavi se sigurnosnim protokolima povezanih uređaja i mreža unutar koncepta IoT. Sigurnost je posebno dobila na važnosti nakon što se pojavio određeni broj incidenata od strane IoT uređaja koji su se do tada često koristili. Stoga je posebnu pažnju trebalo posvetiti zaštiti povjerljivosti podataka i provjeri identiteta, kao dvjema kritičnim točkama. Sigurnost predstavlja jedan od ključnih izazova u budućnosti navedenog koncepta.

# Literatura


[1] Cvitić I. Network Traffic Anomaly Detection Based on Traffic Characteristics and Device Class Affiliation. Sveučilište u Zagrebu, Doktorski rad 2020.

[2] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. IEEE Communications Surveys & Tutorials. 2015;17(4).

[3] Gigli M, Koo S. Internet of Things: Services and Applications Categorization. Advances in Internet of Things. 2011;1(02) 27-31.

[4] Machine-to-Machine (M2M) Communication Challenges Established (U)SIM Card Technology. Preuzeto sa: https://web.archive.org/web/20080107015708/http://www.gi-de.com/portal/page?_pageid=44,139339&_dad=portal&_schema=PORTAL [Pristupljeno: kolovoz 2021.]

[5] Network Traffic Characteristics of the IoT Application Use Cases. Preuzeto sa: https://ecs.wgtn.ac.nz/foswiki/pub/Main/TechnicalReportSeries/IoT_network_technologies_embfonts.pdf [Pristupljeno: kolovoz 2021.]

[6] Žoldin V. Bežične komunikacijske tehnologije za okruženje pametnog grada. Fakultet elektrotehnike, računarstva i informacijskih tehnologija. Osijek. 2017.

[7] Peraković D, Husnjak S, Cvitić I. IoT infrastructure as a basis for new information services in the ITS environment. 22nd Telecommunication Forum. 2014: 39–42.

[8] Angell I, Kietzmann J. RFID AND THE END OF CASH?. COMMUNICATIONS OF THE ACM. 2006;49(12).

[9] ZENSYS' Z-WAVE TECHNOLOGY Preuzeto sa: https://www.pcmag.com/article2/0,2817,1749559,00.asp [Pristupljeno: kolovoz 2021.]

[10] Zigbee Wireless Mesh Networking. Preuzeto sa: https://www.digi.com/solutions/by-technology/zigbee-wireless-standard [Pristupljeno: kolovoz 2021.]

[11] What Is Wi-Fi?. Preuzeto sa: https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html#:~:text=Wi%2DFi%20is%20a%20wireless,to%20interface%20with%20the%20Internet.&text=Internet%20connectivity%20occurs%20through%20a%20wireless%20router [Pristupljeno: kolovoz 2021.]

[12] What is LoRaWAN® Specification. Preuzeto sa: https://lora-alliance.org/about-lorawan/ [Pristupljeno: kolovoz 2021.]

[13] SIGFOX PRESENTS 2017 RESULTS AND 2018 ROADMAP. Preuzeto sa: https://www.sigfox.com/en/news/sigfox-presents-2017-results-and-2018-roadmap [Pristupljeno: kolovoz 2021.]

[14] eMTC (LTE Cat-M1). Preuzeto sa: https://halberdbastion.com/technology/iot/iot-protocols/emtc-lte-cat-m1#:~:text=eMTC%20(enhanced%20Machine%20Type%20Communication,carriers%20existing%20LTE%20base%20stations. [Pristupljeno: kolovoz 2021.]

[15] Internet of Things. Preuzeto sa: https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/ [Pristupljeno: kolovoz 2021.]

[16] Kermek D, Kaniški M, Novak M. Pregled IoT protokola. CASE 28, Rijeka, 2016: 71-78.

[17] The Constrained Application Protocol (CoAP). Preuzeto sa: https://datatracker.ietf.org/doc/html/rfc7252 [Pristupljeno: kolovoz 2021.]

[18] What is MQTT? A practical introduction. Preuzeto sa: https://www.opc-router.com/what-is-mqtt/ [Pristupljeno: kolovoz 2021.]

[19] XMPP. Preuzeto sa: https://en.wikipedia.org/wiki/XMPP [Pristupljeno: kolovoz 2021.]

[20] Advanced Message Queuing Protocol. Preuzeto sa: http://steve.vinoski.net/pdf/IEEE-Advanced_Message_Queuing_Protocol.pdf [Pristupljeno: kolovoz 2021.]

[21] DDS Interoperability Demo. Preuzeto sa: https://web.archive.org/web/20110915193450/http:/www.omg.org/news/meetings/GOV-WS/pr/rte-pres/ddsi-demo.pdf [Pristupljeno: kolovoz 2021.]

[22] Multicast DNS. Preuzeto sa: https://datatracker.ietf.org/doc/html/rfc6762 [Pristupljeno: kolovoz 2021.]

[23] DNS Service Discovery. Preuzeto sa: http://www.dns-sd.org/ [Pristupljeno: kolovoz 2021.]

[24] RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. Preuzeto sa: https://datatracker.ietf.org/doc/html/rfc6550 [Pristupljeno: kolovoz 2021.]

[25] Mulligan G. The 6LoWPAN architecture. Association for Computing Machinery, New York, 2007: 78-82

[26] IEEE Standard for Low-Rate Wireless Networks--Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques. Preuzeto sa: https://standards.ieee.org/project/802_15_4z.html [Pristupljeno: kolovoz 2021.]

[27] Bluetooth Low Energy. Preuzeto sa: https://web.archive.org/web/20170310111443/https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/low-energy [Pristupljeno: kolovoz 2021.]

[28] EPCglobal Preuzeto sa: https://www.gs1.org/epcglobal [Pristupljeno: kolovoz 2021.]

[29] LTE-Advanced (Long Term Evolution-Advanced) preuzeto sa: https://searchmobilecomputing.techtarget.com/definition/LTE-Advanced-Long-Term-Evolution-Advanced#:~:text=Long%20Term%20Evolution%2DAdvanced%20(LTE,per%20second%20over%20LTE%20networks. [Pristupljeno: kolovoz 2021.]

[30] Introduction to IoT security. Preuzeto sa: https://nis-summer-school.enisa.europa.eu/2018/cources/IOT/ENISA_NIS_Summer_School_IoT_Security_1_2018.pdf [Pristupljeno: kolovoz 2021.]

[31] Cvitić I, Vujić M, Husnjak, S. Classification of Security Risks in the IoT Environment. 26-Th Daaam International Symposium on Intelligent Manufacturing and Automation. 2016: 0731–0740.

[32] IoT Security. Preuzeto sa: https://www.slideshare.net/narudomr/iot-security-81762130 [Pristupljeno: kolovoz 2021.]

[33] IoT Security. Preuzeto sa: https://www.slideshare.net/peterwaher/iot-security-117101876 [Pristupljeno: kolovoz 2021.]

[34] Korištenje enkripcije u oblaku i IoT. Preuzeto sa: https://alfatec.hr/2020/06/09/koristenje-enkripcije-u-oblaku-i-iot/ [Pristupljeno: kolovoz 2021.]

[35] Draginic M. Problematika IOT mreže. Tehnički fakultet. Rijeka. 2015.

[36] Imran MA, Zoha A, Zhang L, Abbasi QH. Grand Challenges in IoT and Sensor Networks. James Watt School of Engineering. 2020.

[37] Farhan L, Kaiwartya O, E.Alissa A, Kharel R, Quiroz M, Abdulsalam M. A Concise Review on Internet of Things (IoT) - Problems, Challenges and Opportunities. Budapest, 2018.

# Popis slika

**Slika 1**. IoT elementi ..... 5
**Slika 2**. Arhitektura okruženja pametne zgrade s primjenom koncepta IoT, [1] ..... 12
**Slika 3.** Primjer topologije standarda IEEE 802.15.4 ..... 24
**Slika 4**. IEEE 1905.1 funkcionalnost ..... 25
**Slika 5.** Enkripcija podataka ..... 29

# Popis tablica

**Tablica 1.** Prikaz IoT arhitekture ..... 2
**Tablica 2.** Prikaz IoT elemenata i tehnologija ..... 7
**Tablica 3.** Usluge temeljene na IoT u okviru koncepta pametnoga grada ..... 10
**Tablica 4.** Usporedba tehnologija ..... 20
**Tablica 5.** Prikaz protokola ..... 21
**Tablica 6.** Proširena načela sigurnosti u okruženjima primjene koncepta IoT, [1] ..... 28

# Popis grafikona

Grafikon 1. Predikcija ukupnog broja IoT uređaja do 2025.(globalno), [1] ..... 8
Grafikon 2. Broj povezanih uređaja prema kategorijama, [1] ..... 9

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

## IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Pregled razvoja i primjene bežičnih komunikacijskih tehnologija u području koncepta IoT** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 6.9.2021.

Studentica:

A. S.

*(potpis)*