Analiza izazova i pristupa kod usmjeravanja u mrežama Internet of Things

Perić, Jelena

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

ANALIZA IZAZOVA I PRISTUPA KOD USMJERAVANJA U MREŽAMA *INTERNET OF THINGS*
ANALYSIS OF ROUTING CHALLENGES AND APPROACHES FOR INTERNET OF THINGS NETWORKS

Mentor: prof. dr. sc. Štefica Mrvelj

Student: Jelena Perić
JMBAG: 0135241434

Zagreb, rujan 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Tehnologija telekomunikacijskog prometa II**

DIPLOMSKI ZADATAK br. 6368

Pristupnik: **Jelena Perić (0135241434)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza izazova i pristupa kod usmjeravanja u mrežama Internet of Things**

Opis zadatka:

Prikazati značajke koncepta Internet of Things te mogućnosti njegove primjene. Analizirati izazove koji se pojavljuju kod usmjeravanja prometa u Internet of Things mrežama. Kategorizirati protokole usmjeravanja s obzirom na različite operativne zahtjeve. Analizirati i usporediti performanse protokola koji se koriste za usmjeravanje u IoT mrežama.

Mentor:

Š. Mrvelj

prof. dr. sc. Štefica Mrvelj

Predsjednik povjerenstva za diplomski ispit:

ANALIZA IZAZOVA I PRISTUPA KOD USMJERAVANJA U MREŽAMA INTERNET OF THINGS

SAŽETAK

Cilj ovog diplomskog rada je predstaviti *Internet of Things* koncept te postojeće protokole usmjeravanja koji omogućuju prijenos podataka između povezanih uređaja te analizirati njihove performanse. U radu su detaljno definirane komponente mreža temeljenih na IoT konceptu, karakteristike primijenjenih komunikacijskih tehnologija te mrežna arhitektura. S obzirom na navedeno, prikazana je kategorizacija postojećih područja primjene IoT. Također, definirani su prisutni izazovi prilikom usmjeravanja koji utječu na dizajn i razvoj protokola usmjeravanja te je prikazana klasifikacija protokola usmjeravanja. Shodno tome, opisane su karakteristike postojećih protokola usmjeravanja uz komparativnu analizu definiranih protokola usmjeravanja prema različitim načinima rada i parametrima.

KLJUČNE RIJEČI: Internet of Things; primjena IoT; izazovi usmjeravanja; protokoli usmjeravanja; kategorizacija protokola usmjeravanja;

SUMMARY

This thesis aims to present the Internet of Things concept and existing routing protocols that allow data transfer between connected devices and analyze their performanceS. This thesis defines the components of the IoT concept, the characteristics of the applied communication technologies and its network architecture in detail. Accordingly, the categorization of existing areas of application of IoT is presented. Also, the challenging factors in routing that affect on design and development of routing protocols are defined and the classification of routing protocols is presented. Additionally, the characteristics of existing routing protocols are described with a comparative analysis of defined routing protocols according to different modes of operation and parameters.

KEY WORDS: Internet of Things; Internet of Thing applications; routing challenges; routing protocols; categorization of routing protocols;

SADRŽAJ

1. Uvod

IoT (engl. *Internet of Things*) je koncept, odnosno Internet mreža koja povezuje i omogućuje interakciju između uređaja te između uređaja i čovjeka. Takvu povezanost omogućuju različite tehnologije, kao što su RFID (engl. *Radio-frequency identification*), NFC (engl. *Near-field communication*), senzori, Wifi (engl. *Wireless Fidelity*) i sl.

Postoji niz izazova prilikom usmjeravanja različitih informacija u takvim mrežama koji su istraživani u brojnim radovima, a koji će biti detaljnije obrazloženi i prikazani u diplomskom radu. U IoT konceptu koriste se različite vrste protokola, što je uvjetovano specifičnošću pojedinih mreža, a njihov zadatak je usmjeravanje koje omogućava sigurno i uspješno pristizanje informacija na odredište.

Svrha i ciljevi istraživanja načina usmjeravanja prometa u IoT mrežama bitna je stavka za uspješno funkcioniranje cijelog koncepta, stoga je svrha ovog rada analizirati značajke protokola usmjeravanja u IoT mrežama i razvijenih načina usmjeravanja u njima. U ovom istraživanju naglasak će biti na različitim kategorijama protokola, kao i na njihovim mogućnosti prilikom usmjeravanja.

Glavni ciljevi diplomskog rada su: definirati IoT koncept i njegovu primjenu, analizirati različite izazove prilikom usmjeravanja prometa u takvim mrežama, kategorizirati protokole usmjeravanja s obzirom na različite operativne zahtjeve uređaja te analizirati prednosti i nedostatke protokola usmjeravanja.

Ovaj diplomski rad sastoji se od 7 sljedećih cjelina:

1. Uvod
2. Koncept IoT
3. Mogućnosti primjene IoT koncepta
4. Analiza pristupa kod usmjeravanja prometa u IoT mrežama
5. Kategorizacija protokola usmjeravanja s obzirom na različite operativne zahtjeve
6. Analiza performansi protokola primjenjivih za IoT mreže
7. Zaključak.

U drugom poglavlju rada opisan je i definiran IoT koncept gdje IoT predstavlja novu paradigmu u informacijsko-komunikacijskom svijetu te koji omogućuje interakcije između uređaja i čovjeka i također između uređaja i uređaja. IoT koncept predstavlja rješenje koje se i dalje razvija, shodno tome u ovom poglavlju prikazane su i različite definicije IoT koncepta od strane različitih organizacija. U radu su opisane IoT komponente i arhitektura jer predstavljaju bitan dio i okosnicu navedenog koncepta.

S obzirom na niz prednosti IoT koncepta otvaraju se široke mogućnosti za područja primjene, a mogu se kategorizirati na: primjenu u prometu, logistici i lancima opskrbe, zdravstvu, kućanstvu, prilikom upravljanja energijom, poljoprivredi te na niz ostalih primjena u okruženju. Navedena kategorizacija primjene prikazana je i opisana u trećem poglavlju.

U četvrtom poglavlju prikazani su različiti pristupi i utjecaji na usmjeravanje podataka u IoT mrežama. Veliki broj povezanih uređaja moguć je jedino kroz integraciju različitih tehnologija koje mogu tim uređajima omogućiti da budu identificirani te im pružiti mogućnost međusobne komunikacije. Glavni izazovi koji utječu na usmjeravanje prometa u IoT mrežama bitan su nedostatak IoT mreže, zbog čega je bilo potrebno razviti adekvatna rješenja. Navedena moguća rješenja također se nalaze u ovom poglavlju.

Protokoli koji su primjenjivi u IoT mrežama, mogu se kategorizirati s obzirom na različite operativne zahtjeve, kao što je i prikazano u petom poglavlju. Svaki pojedini protokol ima svoje karakteristike, funkcionalnosti i razloge primjene. S obzirom na izazove koji su definirani u četvrtom poglavlju, u ovom poglavlju navedeni su protokoli koji su dizajnirani na način na koji će zadovoljiti posebne zahtjeve i upotrijebiti različite strategije prilikom usmjeravanja.

Posljednje poglavlje orijentirano je na komparativnu analizu i usporedbu različitih parametara i performansi visoko upotrebljivih protokola usmjeravanja u IoT mrežama.

2. Koncept IoT

IoT koncept može se definirati kao inteligentna globalna mreža koja povezuje sve stvari i uređaje sa svrhom razmijene informacija i komunikacija u skladu s dogovorenim protokolima i standardima. Cilj navedenog koncepta je identifikacija, lociranje, praćenje i upravljanje stvarima. IoT kao rješenje koje se i dalje razvija i raste, nema svoju točnu definiciju. U tablici 1. navedene su definicije IoT koncepta od strane različitih organizacija [1].

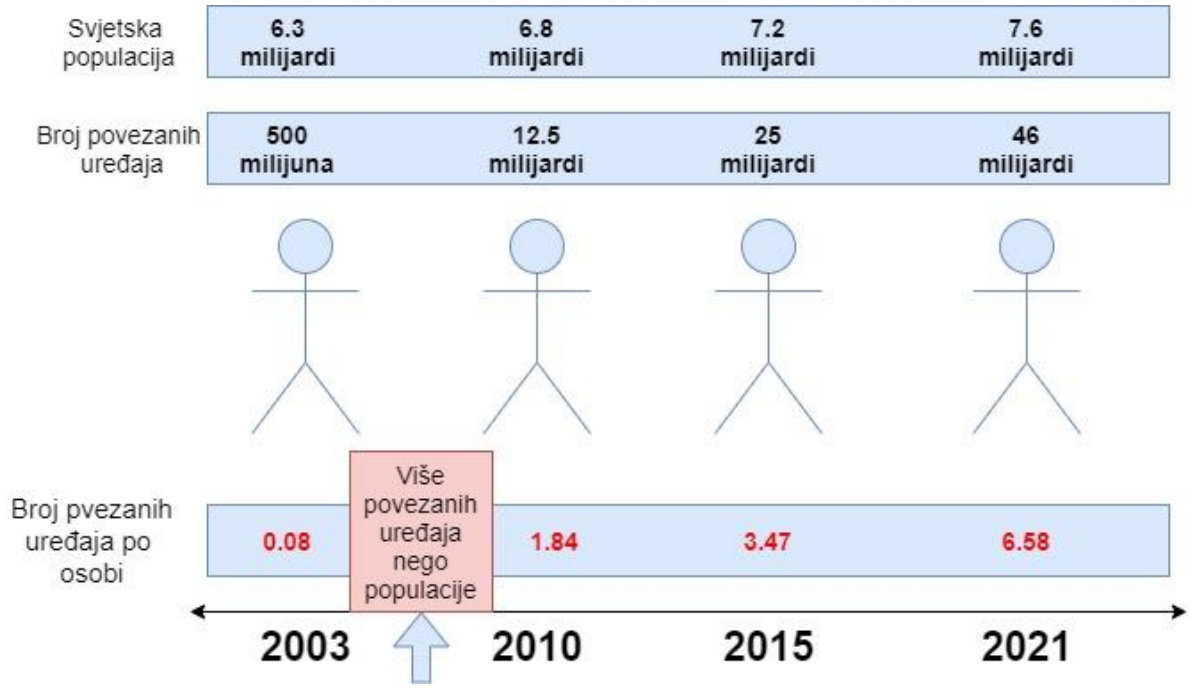
IoT koncept predstavlja novu paradigmu u informacijsko-komunikacijskom svijetu, a omogućuje interakcije između uređaja i čovjeka te između uređaja i uređaja, s ciljem poboljšanja kvalitete života. Osnovna ideja ovog koncepta je povezivanje različitih komunikacijskih tehnologija, bežične komunikacijske mreže, senzora, uređaja i okruženja, kako bi se omogućila komunikacija putem Interneta i generiranje ogromne količine podataka.

Tablica 1. Definicije IoT koncepta od strane različitih organizacija

Organizacije	***Definicije***
CCSA	Mreža koja može prikupljati i kontrolirati informacije i objekte iz fizičkog svijeta putem različitih uređaja sa sposobnošću opažanja, računanja, izvršavanja radnji i komunikacije. Također se smatra mrežom koja podržava komunikacije između uređaja i čovjeka te između uređaja i uređaja, prijenosom, klasifikacijom i obradom informacija.
ITU-T	Globalna infrastruktura za informacijsko društvo koja omogućuje napredne usluge međusobnim povezivanjem virtualnih i fizičkih stvari temeljenih na postojećim informacijsko-komunikacijskim tehnologijama.
EU FP7	Globalna mrežna infrastruktura koja povezuje fizičke i virtualne objekte, iskorištavanjem njihove mogućnosti pohrane podataka i komunikacijskih sposobnosti.
IETF	Svjetska mreža međusobno povezanih objekata koji su jedinstveno adresirani na temelju standardnih komunikacijskih protokola.

Izvor: [1]

Razvoj IoT koncepta i porast broja povezanih uređaja vidljiv je na slici 1. Godine 2003. broj svjetske populacije iznosio je oko 6,3 milijardi, a broj povezanih uređaja na Internet oko 500 milijuna te je iz toga izračunato da je broj uređaja po osobi iznosio 0,08 uređaja. Eksplozivni rast broja povezanih uređaja zabilježen je 2010. godine, a iznosio je 12,5 milijardi. Tada je po prvi put zabilježen veći broj povezanih uređaja nego svjetske populacije, a danas se taj broj već povećao na oko 46 milijardi uređaja [2].



Slika 1. Razvoj Internet of Things-a i broj povezanih uređaja

Izvor: [2]

2.1. Komponente Internet of Things koncepta

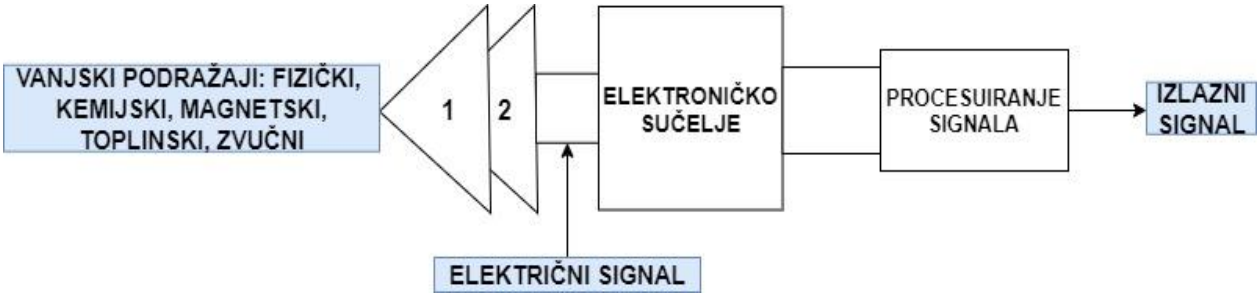
S obzirom na ubrzan rast i razvoj ovog koncepta, bilo je potrebno definirati i samu strukturu, odnosno komponente IoT-a. Na slici 5 prikazano je pet komponenti od kojih se sastoji IoT koncept [3]:

- senzori i aktuatori
- povezivost tj. protokoli i pristupnici
- IoT računalstvo u oblaku
- IoT analitika i upravljanje podacima
- krajnji korisnici i korisnička sučelja.

Okosnicu cijele IoT mreže čine senzori i aktuatori koji su ugrađeni u IoT uređaje te su odgovorni za prikupljanje i upravljanje podacima. Senzori su elektronički uređaji koji se

ponekad nazivaju i detektori jer je njihova primarna funkcija otkrivanje i najmanje fizičke promjene u okruženju zatim tu promjenu pretvaraju u signal koji se može izmjeriti ili snimiti, a struktura senzora prikazana je na slici 2. Prema vrsti vanjskih podražaja senzori se mogu podijeliti na fizički i kemijski senzor, a svi električni pretvarači obično su klasificirani u dvije kategorije tj. pasivni i aktivni. Fizički senzor može se definirati kao uređaj koji reagira na fizičko svojstvo ili podražaj te su zaduženi za proizvodnju odgovarajućih mjerljivih električnih signala. Fizički senzori služi za mjere fizičkih veličina kao što su duljina, temperaturna, električna energija, težina, zvuk itd. Uređaji koji reagiraju na određene kemijske reakcije i koji se mogu koristiti za kvantitativno ili kvalitativno određivanje promjene u okruženju nazivaju se kemijski senzor. Takav se senzor bavi otkrivanjem i mjerenje određene kemijske tvari ili skupa kemikalija. Postoji niz raznolikih vrsta senzora koji su danas dostupni na tržištu, a koriste se za poboljšanje kvalitete ljudskog načina života [4].

Neki IoT uređaji imaju ugrađen veći broj senzora kako bi mogli prikupljati više podataka ili obavljati više funkcija, npr. pametni telefoni sadrže senzor za otisak prsta, senzor za prepoznavanje lica, GPS (engl. *Global Positioning System*), kameru, senzor pokreta i sl. Povećanim razvojem tehnologija, današnji senzori su malih dimenzija, pametni i troškovno isplativi. Odabir senzora ovisi o svrsi koja je potrebna krajnjem korisniku, isto tako izbor senzora ovisi o točnosti i pouzdanosti prikupljenih podataka i rezultata te o razini sposobnosti rada senzora prilikom određenih smetnji (npr. buka, temperatura i sl.). Najčešće korišteni senzori u IoT konceptu su: senzor blizine, senzor za temperaturu, senzor za tlak, optički senzori, senzor za otisak prsta, senzor pokreta, akcelerometar i žiroskop itd.



Slika 2. Struktura senzora

Izvor: [4]

Aktuatori se smatraju mehaničkim pokretačima i rade suprotno od senzora, primaju signale ili naredbe te na temelju njih izvršavaju određene radnje. Aktuatori imaju jednaku važnost u

IoT konceptu kao i senzori jer nakon što senzor detektira promjenu u okruženju, potreban je aktuator koji izvršava radnju [3].

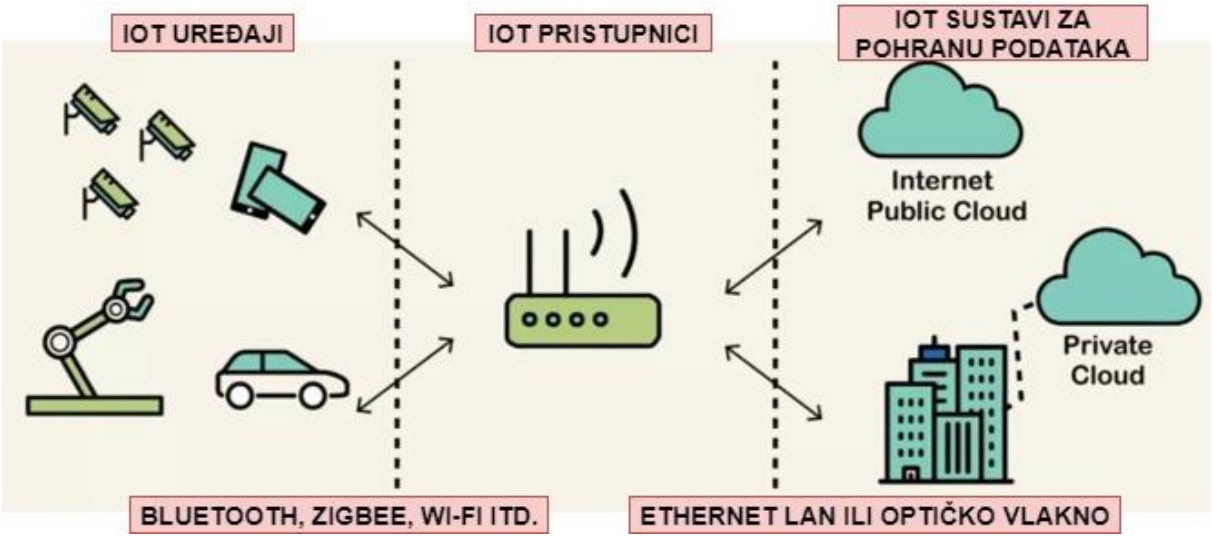
U tipičnom IoT sustavu, senzor je uređaj koji prikuplja informacije te ih usmjerava prema kontrolnom centru, zatim kontrolni centar naredbu šalje aktuatoru koji izvršava radnju, što je vidljivo i na slici 3 [5].

Slika 3. Rad senzora i aktuatora

Izvor: [5]

Sve komponente IoT koncepta moraju biti međusobno povezane kako bi se uspješno prikupljali potrebni podaci i izvršavale zahtijevane radnje.

Drugi dio IoT koncepta čini povezivost tj. protokoli i pristupnici. Nakon što senzori prikupe podatke za prijenos tih podataka do oblaka (engl. *Cloud*) potreban je medij tj. komunikacijski kanal. Protokoli omogućuju komunikaciju između različitih fizičkih objekata i uređaja u IoT mreži, a navedeni su i definirani u petom poglavlju. Dolazni, neobrađeni podaci koje je prikupio senzor, moraju proći kroz pristupnike kako bi stigli do odredišta tj. oblaka, a navedeno u osnovi čini pristupnike ključnom komunikacijskom točkom i odgovornima za upravljanje podatkovnim prometom. Također se mogu smatrati sigurnosnim slojem IoT koncepta jer su podaci koji prolaze pristupnicima zaštićeni. U telekomunikacijama, primarna svrha pristupnika je osigurati poveznicu između različitih komunikacijskih tehnologija, a navedene tehnologije mogu se razlikovati u pogledu vrsta povezivanja, sučelja ili korištenih protokola. Pristupnik je u stvari most između senzora/aktuatora i IoT Clouda te je zadužen za obradu podataka prije slanja. IoT uređaji povezani su s pristupnikom pomoću bežičnih komunikacijskih tehnologija, kao što su Bluetooth, ZigBee, Wi-Fi i sl., a zatim ih povezuje sa IoT računalstvom u oblaku pomoću Ethernet LAN-a ili optičkog vlakna kao što je prikazano na slici 4 [6].



Slika 4. Proces prijenosa podataka od IoT uređaja do Cloud Computinga
Izvor: [6]

Ključne značajke pristupnika IoT-a su [6]:

- premošćivanje komunikacije i M2M komunikacija
- služi kao predmemorija podataka i međuspremnik
- koristi se za izvanmrežne usluge i kontrolu uređaja u stvarnom vremenu
- unaprijed obrađuje, čisti i filtrira podatke prije slanja
- generira ogromne količine podataka prikupljenih od strane senzora
- pruža dodatnu sigurnost
- služi za konfiguraciju uređaja i upravljanje promjenama.

Nakon što su podaci prikupljeni i poslani na odredište tj. u oblak, potrebno ih je obraditi. Integracija IoT-a i računalstva u oblaku proširila je brojne mogućnosti i otvorila vrata različitim domenama primjene koje rukuju s velikim količinama podataka, što je vidljivo u trećem poglavlju. Poznato je da IoT uređaji (senzori, objekti i uređaji) generiraju ogromnu količinu podataka u sekundi. Računalstvo u oblaku pomaže u pohrani i analizi tih podataka tako da korisnici mogu imati maksimalnu korist od IoT infrastrukture. Svojom golemom računalnom snagom, mogućnostima pohrane, mogućnostima umrežavanja, analitikom i drugim uslužnim komponentama, računalstvo u oblaku čini informacije uvijek dostupne korisnicima. IoT rješenje povezuje i omogućuje komunikaciju između stvari, ljudi i procesa. Glavna svrha IoT rješenja pružanje je informacija u stvarnom vremenu, zbog toga mora postojati komponenta sustava koja je u stanju obraditi tako velike količine podataka kako bi se zadovoljila vremenski osjetljiva priroda IoT koncepta. Uređaji, protokoli, pristupnici i pohrana funkcioniraju kao smislena cjelina za učinkovitu analizu podataka u stvarnom vremenu [3].

Zatim slijedi analitički dio koncepta, drugim riječima analitika uključuje pretvaranje velike količine podataka u korisne uvide za daljnja djelovanja u vidu IoT rješenja, zbog toga analitika zahtijeva velike kapacitete skladištenja podataka. Iz tih podataka se mogu konstruirati različita saznanja za predviđanje trendova, planiranje i donošenje korisnih poslovnih odluka.

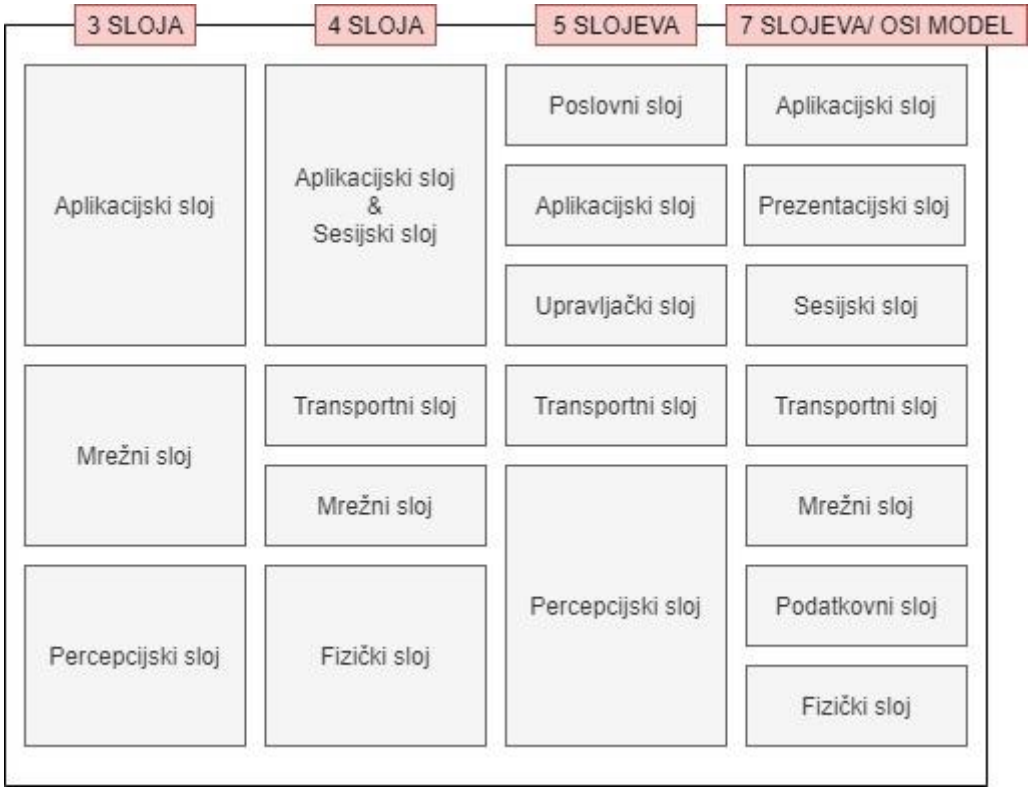
IoT sučelje je vidljiva i posljednja komponenta IoT koncepta, pomoću kojega korisnik može komunicirati i upravljati sustavom. Sučelje bi trebalo biti jednostavnog dizajna i u potpunosti prilagođeno korisniku kako bi se izbjegle bilo kakve poteškoće prilikom korištenja [3].

Slika 5. Komponente Internet of Things koncepta

Izvor: [7]

2.2. Arhitektura Internet of Things koncepta

IoT koncept još uvijek nema standardnu arhitekturu već svaka aplikacija i tehnologija koristi različite složaje za prijenos podataka od izvora do odredišta. Razlog tome je složena struktura sustava, heterogenost povezanih uređaja te skalabilnost mreže. IoT arhitektura mora uključivati uređaje, mreže i aplikacije koji su u međusobnoj interakciji kako bi se korisnicima uspješno isporučivale informacije i usluge. Različiti izvori IoT arhitekturu interpretiraju kroz različit broj slojeva što je prikazano na slici 6, no bitno je naglasiti da su sve predložene arhitekture konstruirane na temelju OSI modela (engl. *Open System Interconnection – Reference Model*) i TCP/IP složaja (engl. *Transmission Control Protocol/ Internet Protocol*). Većina izvora IoT arhitekturu dijeli na četiri sloja, dok su najmanje zastupljene arhitekture one od šest ili sedam slojeva [8].



Slika 6. IoT arhitektura

Izvor: [8]

Slika 7 prikazuje detaljnu arhitekturu IoT koncepta u četiri sloja, a to su sloj uređaja, mrežni sloj, upravljački sloj i aplikacijski sloj. Prema [9], funkcionalnosti svakog sloja opisane su u nastavku.

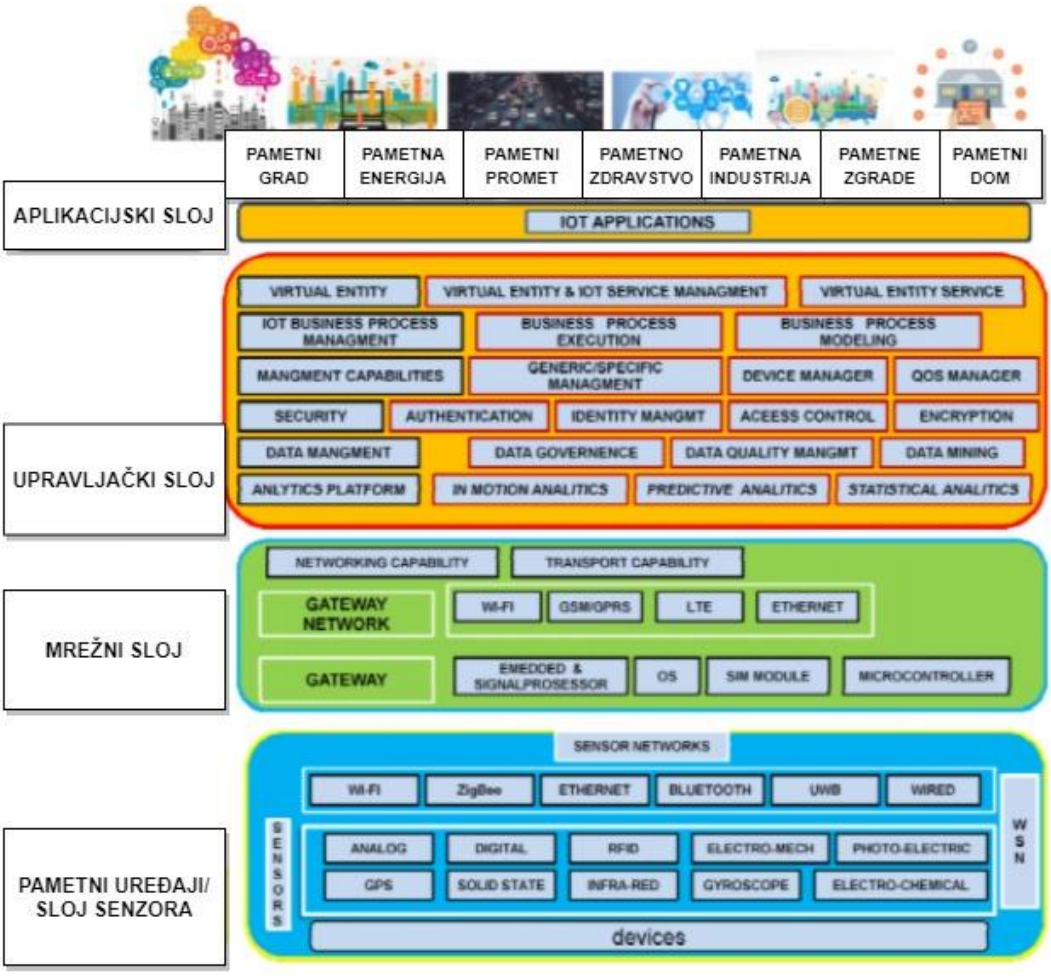
Najniži sloj, sloj uređaja naziva se još sloj senzora, čine ga pametni uređaji povezani sa senzorima i aktuatorima, a senzori su zaduženi za prikupljanje i obradu informacija u stvarnom vremenu. Postoje razne vrste senzora za različite svrhe, pa tako neki od njih imaju sposobnost mjerenja različitih parametara kao što su temperatura, brzina, tlak, vrijeme i sl. Određeni senzori imaju mogućnost zapamtiti i zabilježiti određeni broj mjerenja. Senzori su grupirani prema njihovoj jedinstvenoj namjeni kao što je senzor za okoliš, senzori za tijelo, senzori za kućanske uređaje i vozila itd.

Mrežni sloj se još naziva i transportni sloj. Velika količina podataka bit će proizvedena na nižem sloju od strane senzora koja zahtjeva pouzdanost, sigurnost i visoke performanse mrežne infrastrukture kao prijenosnog medija. Prijenosni mediji mogu biti žične ili bežične mrežne tehnologije gdje su neke od tehnologija 3G, UMTS (engl. *Universal Mobile*

Telecommunications System), 4G, Bluetooth, Wi-Fi i sl. Mrežni sloj prenosi informacije od sloja uređaja do upravljačkog sloja.

Upravljački sloj omogućuje nadzor i obradu informacija u IoT platformi. Navedeni sloj pohranjuje, analizira i obrađuje ogromne količine podataka koji dolaze iz transportnog sloja. On može upravljati nižim slojevima te omogućuje razne usluge kao što su baze podataka, računalstvo u oblaku i moduli za obradu velikih količina podataka.

Aplikacijski sloj nalazi se na samom vrhu arhitekture IoT-a i odgovoran je za dostavu aplikacija korisnicima IoT-a. IoT aplikacije pokrivaju pametna okruženja u različitim područjima primjene, kao što su promet, logistika, zdravstvo i sl. [9].



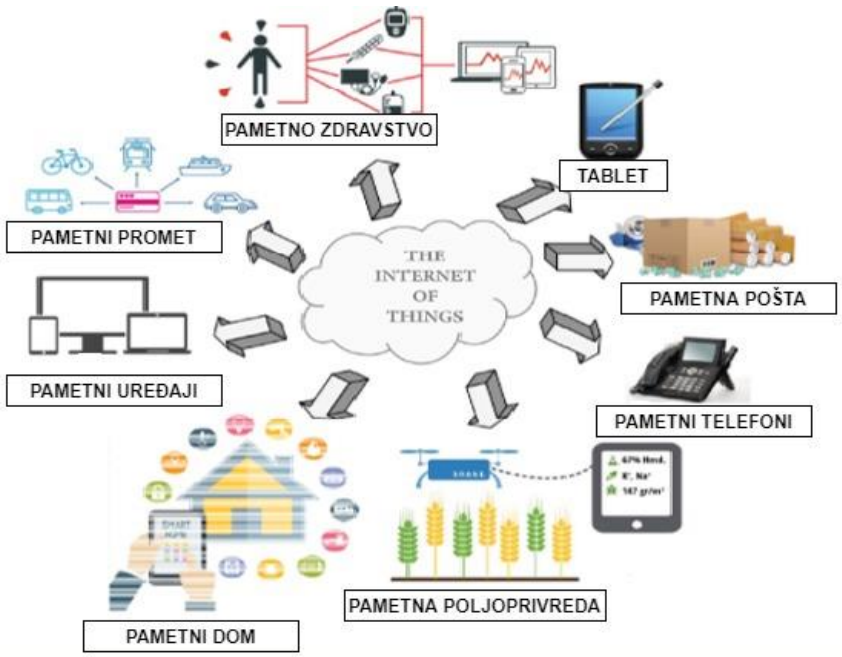
Slika 7. IoT arhitektura kroz četiri sloja

Izvor: [9]

3. Mogućnosti primjene IoT koncepta

IoT koncept temelji se na povezivanju svakodnevno upotrebljavanih uređaja i stvari pomoću Internet mreže. Cilj navedenog koncepta je prikupljanje i obrada informacija iz okoline kako bi krajnji korisnik mogao dobiti pravovremenske informacije. Pojavom IoT koncepta počele su se razvijati nove ideje i ambicije za poboljšanje ljudskog života, koji bi trebao biti pametniji i jednostavniji. Takvi koncepti uključuju pametni promet, pametni lanac opskrbe i logistiku, pametno okruženje, pametno zdravstvo, pametno kućanstvo i pametno upravljanje energijom. Korištenjem IoT koncepta i povezanih tehnologija koje su prikazane u tablici i detaljnije opisane i navedene u 4.3. poglavlju te njihove interakcije s ljudima kao korisnicima otvaraju se široke mogućnosti za područja primjene što je prikazano na slici 8, a mogu se kategorizirati na [10]:

- primjena u prometu
- primjena u logistici i lancu opskrbe
- primjena u zdravstvu
- primjena u kućanstvu
- primjena prilikom upravljanja energijom
- primjena u poljoprivredi
- ostala primjena u okruženju.



Slika 8. Primjena IoT koncepta

Izvor: [11]

Tablica 2. Korištene tehnologije u domenama primjene IoT koncepta

Područje primjene	*LPWAN*	*ZigBee*	*Bluetooth*	*Wi-Fi*	*RFID*
Industrija	❖	❖			
Zdravstvo			❖	❖	
Upravljanje energijom	❖				
Kućanstvo	❖	❖	❖	❖	
Logistika	❖				❖
Poljoprivreda	❖				
Promet	❖		❖	❖	

Izvor: [12]

3.1. Primjena u prometu

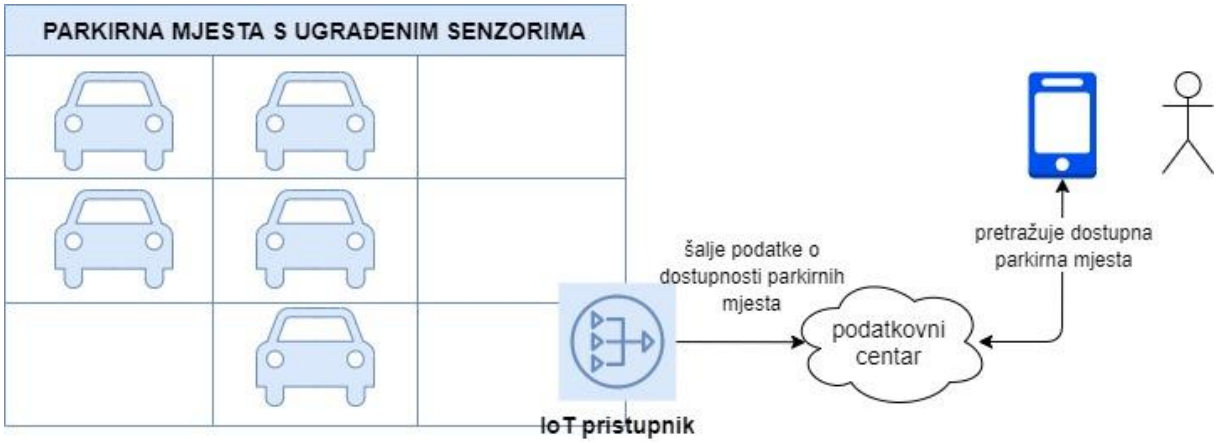
IoT koncept je pripomogao stvoriti mnoge transportne usluge te je unaprijedio već postojeće. Aplikacije vezane za primjenu u prometu mogu upravljati dnevnim prometom u gradovima pomoću senzora i inteligentnih sustava za obradu informacija. Glavni ciljevi inteligentnih transportnih sustava i aplikacija usmjereni su na smanjivanje svakodnevnih prometnih gužvi, izbjegavanje prometnih nesreća pravilnim usmjeravanjem prometa te na jednostavno parkiranje bez ometanja drugih vozila. Način na koji IoT koncept regulira parking i obavještava korisnike o dostupnosti parkirnih mjesta, prikazan je na slici 9. Senzorske tehnologije koje upravljaju ovom vrstom aplikacija su GPS senzori za lokaciju, akcelerometri za brzinu, žiroskopi za smjer, RFID za identifikaciju vozila te kamere za snimanje kretanja vozila i prometa [10].

Moguće je izdvojiti nekoliko aplikacija koje se koriste u ovom sektoru:

- Aplikacije za nadzor i upravljanje vozilom gdje su vozila međusobno povezana mrežom, računalstvom u oblaku i mnoštvom IoT uređaja poput GPS senzora, RFID uređaja i kamera. Otkrivanje povećanog prometa tj. zagušenja omogućeno je pomoću senzora za pametne telefone, poput akcelerometra i GPS senzora. Ovisno o trenutnoj lokaciji vozila, aplikacije obavještavaju vozača o stanju na cestama te u slučaju povećane gustoće prometa, vozaču predlažu alternativne puteve.
- Aplikacije vezane za sigurnost podrazumijevaju tehnologije detekcije lica, detekcije pokreta očiju i detekcije pritiska na upravljaču, pomoću kojih se promatra stanje

vozača. U slučaju detekcije umora vozača, aplikacije za sigurnost vozaču predlažu odmor. Navedene tehnologije povećavaju sigurnost vožnje.

- Aplikacije za pametni parking šalju informacije korisnicima o dostupnosti najbližih slobodnih parkirnih mjesta te se na taj način smanjuje vrijeme traženje parkirnog mjesta.
- Aplikacije za pametno upravljanje semaforima služe za regulaciju prometnih gužvi na raskrižjima u svakom smjeru. Prikupljene informacije uglavnom se prosljeđuju susjednim semaforima kako bi promet bio u potpunosti usklađen i bez zagušenja. Tehnologije koje je se koriste za ovaj način upravljanja semaforima su kamere, komunikacijske tehnologije i moduli za analizu podataka.
- Aplikacije za određivanje mjesta nesreće nalaze se na pametnom telefonu ili u samom vozilu te u trenutku nesreće šalju informacije hitnim medicinskim službama.

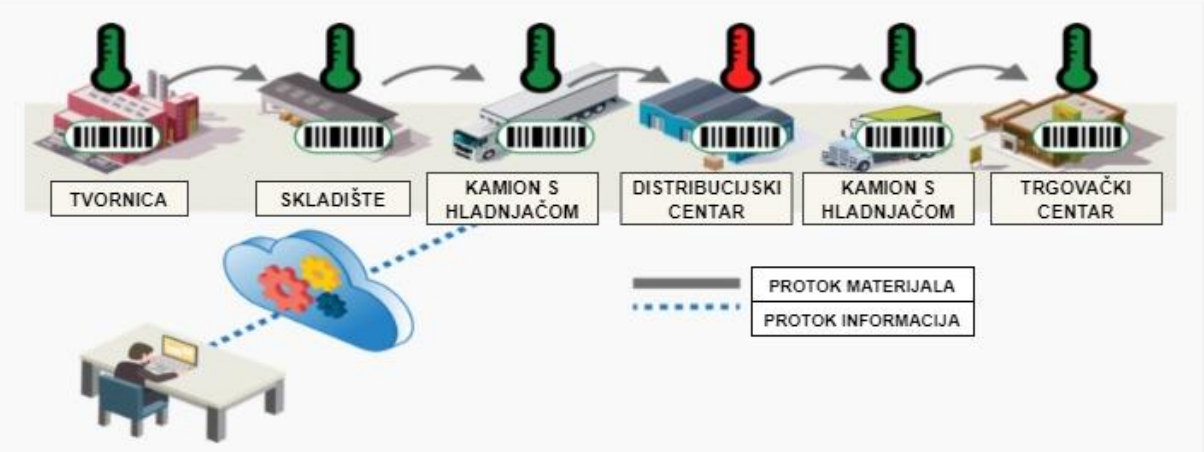


Slika 9. IoT pametni parking
Izvor: [10]

3.2. Primjena u logistici i lancu opskrbe

IoT paradigma pokušava pojednostaviti procese nabave i prijenosa potrebnih resursa i robe pomoću pametnih aplikacija i informacijskih sustava. Roba u opskrbnom lancu može se lako pratiti od mjesta proizvodnje do odredišne točke distribucije pomoću senzorskih tehnologija kao što su RFID i NFC, način na koji funkcionira primjena i prijenos proizvoda u IoT-u prikazan je i na slici 10. Stvarnovremenske informacije i podaci koji se zapisuju i analiziraju vezani su uz kvalitetu proizvoda i prijenosa, količinu proizvoda, put usmjeravanja, trenutnu lokaciju robe i sl. Sustav prijenosa informacija koji služi za upravljanje lancem opskrbe koristi RFID oznake za identifikaciju proizvoda, te se na taj način stvara mreža informacija o proizvodima koji se

prenose. Automatsko prikupljanje informacija o proizvodima također služi za prognoziranje budućnosti u vidu ponude i potražnje. IoT koncept na ovaj način dugoročno poboljšava performanse sustava opskrbnog lanca [10].



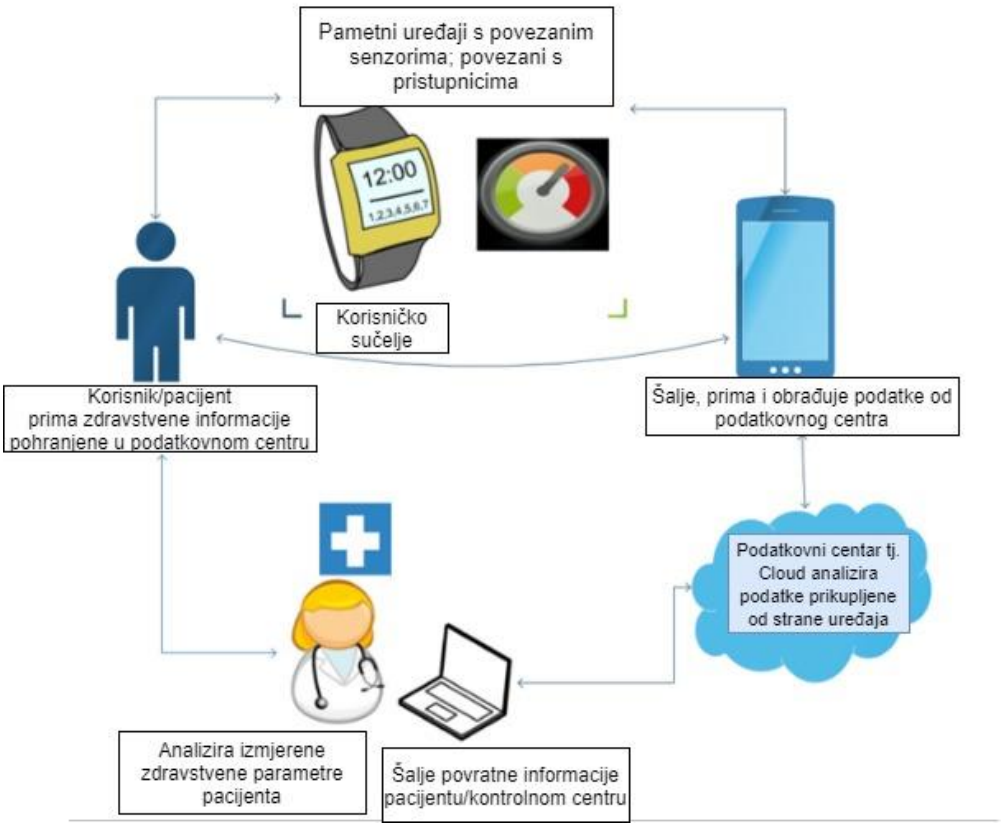
Slika 10. Primjena IoT koncepta u logistici i lancu opskrbe
Izvor: [13]

3.3. Primjena u zdravstvu

IoT aplikacije u sektoru zdravlja pokazale su svoju učinkovitost korištenjem nosivih uređaja koji prate zdravstveno stanje osobe, što je vidljivo na slici 11. Navedene aplikacije omogućuju neovisan život starijim osobama i pacijentima sa zdravstvenim problemima. Trenutno, IoT senzori kontinuirano prate i zapisuju zdravstveno stanje pacijenta. Nadzor i izvještavanje u stvarnom vremenu putem povezanih uređaja mogu spasiti živote u slučaju potrebe za hitnom medicinskom pomoći, poput napada astme, prekomjerne razine šećera, srčanih i moždanih udara i sl.

IoT uređaji i povezane tehnologije omogućuju praćenje tjelesne temperature osobe, otkucaje srca, krvni tlak i sl. IoT uređaji na taj način kreiraju elektronički zdravstveni zapis pacijenta koji je uvijek dostupan.

Zdravstveni sektor jedan je od najkritičnijih sektora koji koristi pojedinac te je potrebno poboljšati zdravstvene usluge i smanjiti materijalne troškove pojedinca i ustanove. Sve navedeno omogućuje IoT koncept tj. poboljšava upravljanje, analizu i obradu podataka na svim razinama zdravstva [14].

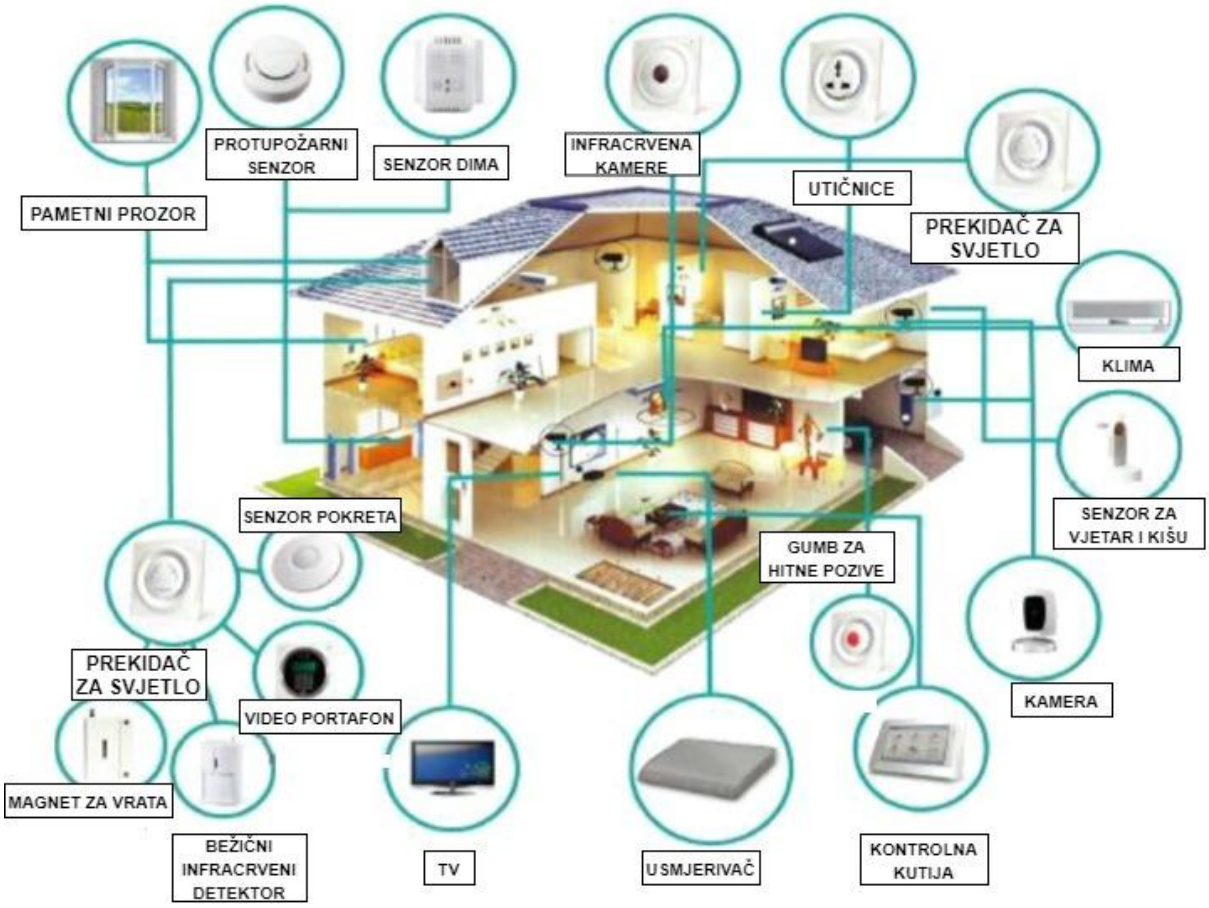


Slika 11. Primjena IoT u zdravstvu

Izvor: [10]

3.4. Primjena u kućanstvu

Primjena IoT koncepta u kućanstvu podrazumijeva prebivalište opremljeno informacijsko-komunikacijskom mrežom, visokotehnološkim kućanskim uređajima te senzorima koji pružaju usluge po potrebi ukućana. Neke od usluga pametnog doma podrazumijevaju upravljanje rasvjetom, regulaciju grijanja i klimatizacije pomoću termostata povezanog na mobilnu aplikaciju, aktivaciju alarma, podizanje i spuštanje roleta ovisno o dobu dana, elektromehaničke brave koje se otključavaju i zaključavaju pomoću otiska prsta ili lozinke i sl. Sve navedeno omogućeno je povezanosti različitih dijelova kućanstva u jednu mrežnu cjelinu koja ima pristup Internetu, što je prikazano i na slici 12 [10].



Slika 12. Primjena IoT u kućanstvu

Izvor: [10]

3.5. Primjena prilikom upravljanja energijom

Pametna energetska mreža je informacijsko-komunikacijska tehnologija koja omogućuje suvremeni sustav proizvodnje, prijenosa, distribucije i potrošnje električne energije te kontrolira i optimizira protok električne energije.

Aplikacija koja se najčešće koristi u ovom sektoru je pametno brojilo koje služi za očitavanje i analizu potrošnje električne energije. Zatim se ti podaci šalju poslužitelju, a također su dostupni i korisniku električne energije. Pomoću tih dostupnih podataka i zapisa o potrošnji korisnik može u budućnosti smanjiti troškove tj. potrošnju električne energije.

Pametni uređaji za nadzor energije također su bitna stavka ove mreže, a u tablici 3 jasno su vidljive napredne značajke pametnog uređaja za nadzor energije u odnosu na tradicionalni uređaja za nadzor energije. Tradicionalni uređaj ograničenih je mogućnosti te primjenjuje samo jednosmjernu komunikaciju od uređaja do kontrolnog centra, dok pametni uređaj omogućuje dvosmjernu komunikaciju tj. od pametnog uređaja do kontrolnog centra i obratno. Pametni uređaji sposobni su upravljati potrošačkim opterećenjem te šalju obavijesti kontrolnom centru

prilikom neovlaštenih događaja kako bi se poduzele odgovarajuće radnje, dok tradicionalni uređaj nema navedene sposobnosti [10].

Tablica 3. Usporedba tradicionalnog i pametnog uređaja za nadzor energije

Tradicionalni uređaj za nadzor energije	*Pametni uređaj za nadzor energije*
• Jednosmjerna komunikacija, od nadzornog uređaja do kontrolnog centra	• Dvosmjerna komunikacija, od pametnog nadzornog uređaja do kontrolnog centra i obratno
• Nije u mogućnosti upravljati potrošačkim opterećenjem	• Sposoban je upravljati potrošačkim opterećenjem
• Ne šalje obavijesti/alarme prilikom određenih događaja u mreži	• Šalje obavijesti/alarme prilikom određenih događaja u mreži
• Podržava nadzor energije u jednom smjeru, tj. samo uvoz energije	• Podržava nadzor energije u oba smjera, tj. uvoz i izvoz energije
• Podržava samo automatizacijske protokole ograničenih mogućnosti	• Podržava automatizaciju, nadzor energije i komunikacijske protokole

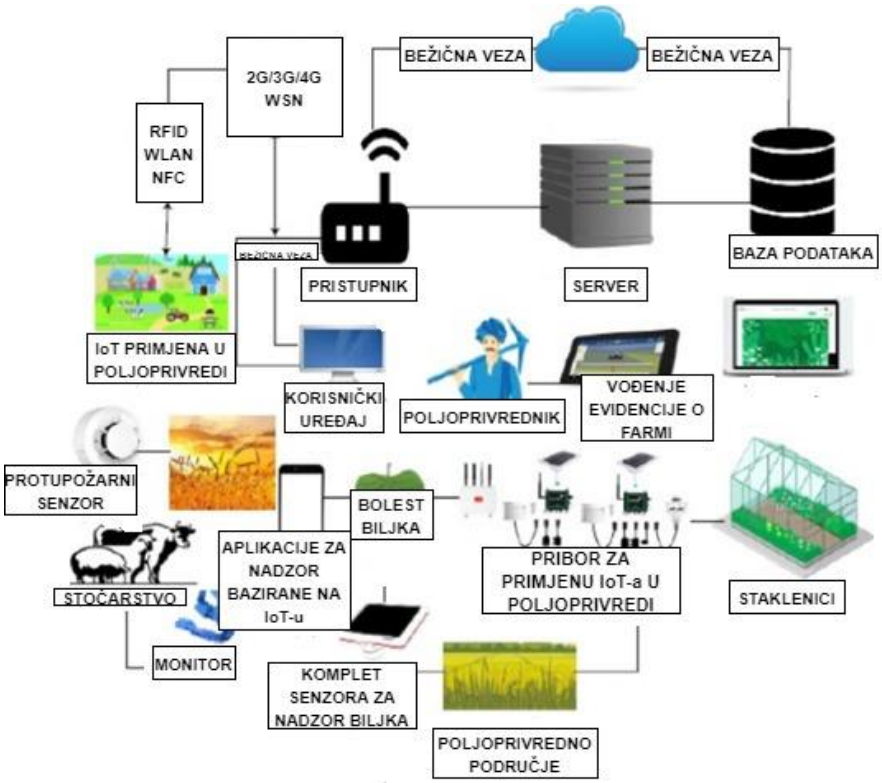
Izvor: [15]

3.6. Primjena u poljoprivredi

Parametri okoliša, poput temperature, vlažnosti zraka, količine sunčevog zračenja, podataka o stanju tla i sl., bitna su stavka za uspješnu poljoprivrednu proizvodnju, zbog toga poljoprivrednici koriste senzore za mjerenje navedenih parametara u stvarnom vremenu, a rezultati i prikupljeni podaci se koriste za poboljšanje kvalitete uzgoja. Jedna od bitnih IoT aplikacija koju poljoprivrednici koriste, služi za automatsko navodnjavanje površina ovisno o vremenskim uvjetima. Podaci sa terena prikupljeni senzorima mogu pomoći u postizanju visoke razine točnosti u proračunu potrebe tla za vodom, a navedeno povećava količinu proizvodnje i profit te optimizira količinu utrošene vode i energije. Proizvodnja pomoću staklenika također je jedna od glavnih primjena IoT-a u poljoprivredi.

Cijeli IoT sustav namijenjen primjeni u poljoprivredi je učinkovit, napredan, pouzdan i praktičan te doprinosi ostvarenju cilja svakog poljoprivrednika. Isto tako povećava se produktivnost i globalno tržište te se smanjuje ljudska intervencija, vrijeme i troškovi [16].

Jedan od primjera primjene IoT-a u poljoprivredi prikazan je na slici 13.



Slika 13. IoT primjena u poljoprivredi

Izvor: [17]

4. Analiza pristupa kod usmjeravanja prometa u IoT mrežama

Postupak usmjeravanja u IoT mrežama odnosi se na odabir puta prijenosa informacija od izvora do odredišta, a glavni ciljevi usmjeravanja svode se na održavanje integriteta prenesenih podataka i uspješan dolazak na odredište. S obzirom na navedena ograničenja i izazove u 4.1. poglavlju prilikom usmjeravanja potrebno je optimalno iskoristiti mrežne resurse. Postoje različiti pristupi i načini usmjeravanja koji su primjenjivi za IoT mreže, a definirani su u 4.3. poglavlju, s povezanim prednostima i nedostatcima. Različiti načini usmjeravanja zahtijevaju i niz raznovrsnih tehnologija koje se nalaze u 4.2. poglavlju. Navedene tehnologije mogu u velikoj mjeri olakšati proces usmjeravanja podataka u IoT mrežama, no mogu i otežati zbog svoje raznovrsnosti te različitog načina rada.

4.1. Izazovi u usmjeravanju prometa u IoT mrežama

Svrha IoT koncepta je poboljšanje kvalitete života čovjeka, no za ostvarivanje navedenog potrebno je savladati određene prepreke te naći rješenja za određene izazove. U nastavku su navedeni glavni izazovi koji utječu na usmjeravanje prometa u IoT mrežama.

1. Ograničeni resursi predstavljaju jedan od glavnih izazova IoT-a. Navedeni resursi uključuju opskrbu uređaja energijom, procesorsku snagu uređaja, kapacitet memorije uređaja, domet bežične komunikacije i propusnost bežične komunikacije. Ova ograničenja stvaraju različite prepreke prilikom usmjeravanja prometa.

   Kratkodometne bežične komunikacije zahtijevaju usmjeravanje u kojem podatkovni paketi moraju biti proslijeđeni na više posredničkih čvorova kako bi stigli na odredište. Zatim, nedostatna procesorska snaga i ograničeni programski kapacitet memorije zahtijevaju optimiziran proces usmjeravanja koji se izvodi na IoT uređajima. Nedovoljna memorija za pohranu i propusnost bežične komunikacije ograničavaju veličinu paketa za prosljeđivanje. Također prilikom usmjeravanja, ograničeni izvori energije otežavaju odabir čvorova za prosljeđivanje podatkovnih paketa, pošto bežična komunikacija troši velike količine energije IoT uređaja [18].
2. Izazov prilikom usmjeravanja prometa u IoT mrežama također je i dinamična topologija mreže u kojoj se usmjerava promet. Za razliku od tradicionalne mreže u kojoj je topologija mreže bila unaprijed definirana, u IoT mreži jako je teško održat topologiju fiksnom. Razlog tome mogu biti nasumično raspoređeni čvorovi u mreži, kvarovi na čvorovima, nedovoljno trajanje baterije uređaja i sl. Isto tako, IoT uređaji isključivanjem uređaja za odašiljanje signala smanjuju potrošnju energije čime uzrokuju

dinamičnost topologije ove mreže. Stoga protokoli usmjeravanja moraju biti dovoljno fleksibilni kako bi se uspješno nosili s dinamičnošću topologije IoT-a [19].

3. IoT platforma povezuje različite vrste tehnologija i uređaja. Povezani uređaji se razlikuju prema vrsti mrežnih standarda koje koriste i vrsti aplikacija koje podržavaju, a povezane tehnologije su npr. tradicionalna mreža, WSN (engl. *Wireless Sensor Network*), Zigbee, WiFi itd. Načela rada ovih tehnologija su raznolika, koriste različite protokole usmjeravanja. Sve navedeno otežava proces usmjeravanja prometa u IoT mrežama [20].
4. Izazov usmjeravanju u IoT-u isto tako može biti prisutnost mrežnih pregrada i praznina. Pregrada predstavlja nepovezani dio mreže, što znači da čvorovi koji se nalaze unutar pregrade ne mogu komunicirati s čvorovima koji se nalaze u ostalim dijelovima mreže, jer ne postoji definirani put usmjeravanja za razmjenu podatkovnih paketa s dijelovima koji nisu povezani s mrežom. Praznina također nije obuhvaćena mrežom te unutar nje nema čvora koji je povezan s čvorovima u mreži, stoga se podatkovni paketi prosljeđuju samo čvorovima oko praznine kako bi stigli do svog odredišta [21].
5. IoT je korisnicima omogućio brojne prednosti u korištenju, no samim time i određene izazove u sigurnosti i privatnosti njihovih podataka. Kibernetički napadi pokazali su se kao jedna od glavnih ranjivosti ovog sustava prilikom usmjeravanja, a od svih gore navedenih izazova niti jedan nema tako značajan utjecaj na IoT poput sigurnosti i privatnosti podataka. Obično se IoT mreža sastoji od skupa sličnih ili gotovo identičnih uređaja koji imaju slične karakteristike, a upravo to povećava ranjivost. Posljedica nedovoljne zaštite i adekvatnih sigurnosnih mjera nad podacima uglavnom se svodi na gubitak bitnih podataka [22].
6. S obzirom na niz čimbenika koji utječu na okruženje IoT koncepta, uvijek postoji opasnost utjecaja tih čimbenika na ukupne performanse mreže. Što znači da protokoli usmjeravanja moraju imati ugrađene mehanizme koji podržavaju neočekivane događaje u mreži tj. moraju imati visoku toleranciju na pogreške, u suprotnom to može biti značajan nedostatak i ograničenje prilikom usmjeravanja. Takvi neočekivani događaji mogu utjecati i na pravovremenu isporuku informacija, a kašnjenje uvelike može smanjiti kvalitetu usluge te prouzročiti niz problema korisnicima [23].
7. Prilikom usmjeravanja čvorovi su u mogućnosti detektirati višak podataka koji se prenosi mrežom. U senzorskim mrežama se do krajnjeg odredišta ne šalju svi podaci prikupljeni od različitih čvorova, nego se vrši agregacija tih podataka, prema tome, podaci koji se smatraju suvišnima, moraju se ukloniti prije pristizanja na odredište.

Tehnika otkrivanja nepotrebnih paketa i podataka naziva se agregacija podataka, a njen cilj je smanjiti složenost podataka koji se prenose te objediniti samo one korisne. Na taj se način postiže visoka energetska učinkovitost te se štedi ograničenost resursa.

Većina sustava i algoritama koji se koriste za agregaciju podataka nemaju u sebi implementirane sigurnosne mehanizme te su kao takvi podložni različitim vrstama napada, a najčešće je riječ o dodavanju lažnih informacija i podataka prilikom same agregacije [23].

8. IoT sustav povezuje veliku količinu tehnologija koje su detaljnije razrađene u poglavlju 4.1., senzora, aktuatora i drugih uređaja sa sposobnošću razmjene informacija i velikog broj aplikacija putem interneta, što može utjecati na veličinu same mreže. Zbog toga je bitno dizajnirati sustav koji će biti sposoban podnositi promjene u opsegu mreže i broju povezanih uređaja. Skalabilnost je sposobnost mreže da se prilagodi promjenama u okruženju, a također utječe na usmjeravanje u IoT mreži, jer usmjeravanje znači odlučiti kojim putem je potrebno poslati paket kako bi on stigao na željeno odredište, što je više uređaja i čvorova u mreži to je usmjeravanje složenije. Pretpostavlja se da će složenost mreže rasti te je zbog toga potrebno dizajnirati protokole usmjeravanja koji će podnositi izazov skalabilnosti mreže [21].

4.2. Korištene tehnologije u IoT konceptu

Razvoj sveprisutnog računalnog sustava gdje se digitalni objekti mogu jedinstveno identificirati i mogu razmišljati te imati interakciju s drugim objektima kako bi prikupljali podatke na temelju kojih se poduzimaju automatizirane radnje zahtijeva kombinaciju nove i učinkovite tehnologije. Navedeno je moguće jedino kroz integraciju različitih tehnologija koje mogu objektima omogućiti da budu identificirani te im pružiti mogućnost međusobne komunikacije [24]. U ovom odjeljku navedene su tehnologije koje mogu u velikoj mjeri pomoći u razvoju IoT-a, no mogu i otežati zbog sove raznolikosti te različitog načina rada, što je i navedeno kao izazov prilikom usmjeravanja u prethodnom poglavlju.

4.2.1. RFID

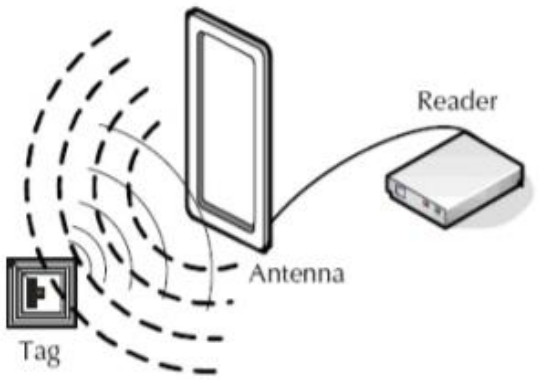
RFID je ključna tehnologija za jedinstveno prepoznavanje objekata. Zbog male veličine, ali i cijene, može biti integriran u bilo koji uređaj. Riječ je o primopredajnom mikročipu sličnom ljepljivoj naljepnici koji može biti aktivan ili pasivan, ovisno o vrsti primjene.

Aktivne oznake imaju priključenu bateriju zbog koje su uvijek aktivni te tako kontinuirano emitiraju podatkovni signali dok se pasivne oznake aktiviraju samo kada je potrebno. Aktivne

oznake su skuplje od pasivnih, ali bez obzira na to imaju širok raspon korisnih primjena. RFID sustav je sastavljen od čitača i pripadajućih RFID oznaka koje emitiraju identifikaciju, lokaciju ili bilo koju drugu specifikaciju objekta što je prikazano na slici 14, nakon što ih pokrene generiranje odgovarajućeg signala. Emitirani podaci povezani s objektima prenose se čitačima pomoću radio frekvencija koje se zatim prosljeđuju na procesore za analizu podataka. Ovisno o vrsti aplikacije, RFID frekvencije se dijele u 4 različita frekvencijska raspona, koja su dana u nastavku:

1. niska frekvencija (135 KHz ili manje)
2. visoka frekvencija (13,56 MHz)
3. izuzetno visoke frekvencije (862 MHz 928 MHz)
4. frekvencija mikrovalne pećnice (2.4 G, 5.80).

QR (engl. *Quick Response code*) kod je također tehnologija identifikacije koja ima gotovo istu funkciju kao RFID, ali je RFID učinkovitiji od QR koda zbog niza prednosti. RFID kao radio tehnologija ne zahtijeva fizičku prisutnost čitača dok je QR kod optička tehnologija koja ne može funkcionirati ukoliko čitač nije postavljen ispred njega. RFID može raditi kao pokretač za različite događaje, a također ima mogućnosti modifikacije koje QR kodovi nemaju [24].



Slika 14. Način rada RFID tehnologije
Izvor: [24]

4.2.2. WSN

WSN je dvosmjerna bežično povezana mreža senzora u multi-hop načinu, izgrađena od nekoliko čvorova raspršenih u senzorskom polju, svaki povezan s jednim ili više senzora koji mogu prikupljati podatke specifične za svaki objekt poput temperature, vlage, brzine itd. a zatim proslijediti podatke do opreme za obradu. Senzorski čvorovi komuniciraju u više skokova.

Svaki senzor je primopredajnik koji ima antenu, mikrokontroler i sklop za povezivanje senzora za komunikaciju, aktivacijsku i senzorsku jedinicu s izvorom energije koji može biti i baterija ili bilo koja tehnologija koja crpi energiju. Dodatna jedinica za spremanje podataka naziva se memorijska jedinica koja također može biti dio senzorskog čvora.
Kombinacijom WSN i RIFD tehnologija otvara se mogućnost za više pametnih uređaj [24].

4.2.3. Cloud Computing

S milijunima uređaja koji se tek trebaju pojaviti, računalstvo u oblaku se smatra jedinom tehnologijom koja može analizirati i pohraniti sve potrebne podatke. Računalstvo u oblaku smatra se inteligentnom računalnom tehnologijom u kojoj broj poslužitelja konvergira na jednoj cloud platformi kako bi omogućila dijeljenje podataka kojima se može pristupiti bilo kada i bilo gdje. Računalstvo u oblaku je najvažniji dio IoT-a jer omogućuje velike kapacitete pohrane podataka te kada se poveže s pametnim objektima koji su prikazani na slici 15 koristeći veliki broj potencijalnih senzora od njega se može izvući još veća korist, a samim time doprinosi razvoju IoT mreže [24].

Slika 15. Cloud Computing i povezani uređaji
Izvor [24]

4.2.4. Mrežne tehnologije

Mrežne tehnologije imaju važnu ulogu u uspjehu razvoja IoT-a od kad su odgovorne za povezanost između objekata, zbog toga je potrebna brza i učinkovita mreža kako bi mogla podnijeti veliki broj potencijalnih uređaja. Za velike domete prijenosne mreže uobičajeno koriste 3G/4G/5G tehnologije. Na primjer, mobilni promet je predvidljiv budući da mora izvršavati samo uobičajene zadatke kao što su slanje tekstualnih poruka ili uspostava poziva.

Dok se za komunikacije kratkog dometa koriste tehnologije poput LPWAN, Bluetooth, WiFi, ZigBee, NFC i sl. [24].

Tablica 4 uspoređuje komunikacijske mrežne tehnologije s obzirom na korištenu mrežu, topologiju, količinu potrošnje energije uređaja, brzinu i domet [25].

Tablica 4. Specifikacije IoT korištenih tehnologija

	RFID	*NFC*	*Wi-Fi*	*ZigBee*	*Bluetooth*	*WSN*
Mreža	PAN	PAN	LAN	LAN	PAN	LAN
Topologija	od točke do točke	od točke do točke	zvjezdasta	stablasta, isprepletena, zvjezdasta	zvjezdasta	isprepletena, zvjezdasta
Potrebna energija	vrlo niska	vrlo niska	varira od niske do visoke	vrlo niska	niska	vrlo niska
Brzina prijenosa	400 kbs	400 kbs	11-10 Mbs	250 kbs	700 kbs	250 kbs
Domet	< 3 m	< 0.1 m	4-20 m	10-100 m	<30 m	200 m

Izvor: [25]

4.2.5. Nano-tehnologije

Nano tehnologije služe za povezivanje manjih uređaja čije se dimenzije mogu izraziti u nanometrima, a mogu se koristiti kao senzori ili pokretači u IoT mrežama baš kao normalni uređaji. Također, navedeni uređaji mogu smanjiti energetsku potrošnju sustava te se sastoje od nano-komponenti što rezultira definiranjem nove mreže koja se naziva *Internet of Nano-Things*.

4.2.6. Mikro-elektro-mehanički sustavi

Mikro-elektro-mehanički sustavi MEMS (engl. *Micro-Electro-Mechanical Systems*) su kombinacija električnih i mehaničkih komponenti koje rade zajedno kako bi pružile više mogućih primjena, uključujući očitavanje senzora i aktivaciju. U mrežama se koriste već u obliku pretvarača i akcelerometra. MEMS u kombinaciji s nano-tehnologijama nudi isplativo rješenje za improviziranje komunikacijskog sustava IoT-a, ali i ostale prednosti poput smanjenja veličine senzora, integriranih sveprisutnih računalnih uređaja, većeg raspona frekvencija itd.

4.3. Načini usmjeravanja u IoT mrežama

Usmjeravanje je ključna usluga u IoT mrežama između povezanih objekata. Učinkovito usmjeravanje podrazumijeva pouzdanu isporuku podataka od izvora do odredišta. Zbog velikog broja povezanih objekata, dinamične topologije IoT mreže te ograničenih resursa IoT uređaja, usmjeravanje predstavlja izazov za ovu mrežu. Načini usmjeravanja koji se koriste u IoT mrežama se mogu podijeliti na centralizirani i distribuirani način usmjeravanja, usmjeravanje temeljeno na podatcima i temeljeno na adresi, usmjeravanje temeljeno na lokaciji i temeljeno na stanju te istorazinsko i hijerarhijsko usmjeravanje, a u nastavku su definirani te su navedene njihove prednosti i nedostatci [21].

4.3.1. Centralizirani i distribuirani način usmjeravanja

Centralizirani i distribuirani načini usmjeravanja odnosi se na mjesto odluke o usmjeravanju, odnosno odluke o odabiru puta usmjeravanja paketa. Centralizirani način usmjeravanja temelji se na glavnom čvoru za kojeg se pretpostavlja da ima dovoljno resursa i znanja o stanju mreže da može kontrolirati cijelu mrežu. Glavni čvor ima kontrolu nad svim ostalim čvorovima u mreži i određuje optimalni put usmjeravanja za svaki paket. Prednost centraliziranog usmjeravanja je kompletna kontrola nad cijelom mrežom i sigurnost prenesenih podataka. Pod nedostatke se navodi skupo održavanje glavnog čvora zbog količine zadataka koje mora dodijeliti svakom čvoru u mreži te prilikom kvara na glavnom čvoru, cijela mreža prestaje funkcionirati. Zbog dinamičnosti topologije IoT mreže, centralizirani način usmjeravanja često mora određivati nove rute.

U distribuiranom načinu usmjeravanja odluku o usmjeravanju donosi svaki čvor za sebe ili grupa čvorova. Čvorovi nemaju pregled nad cijelom mrežom. Odluka o usmjeravanju se definira na temelju ograničenog znanja o stanju mreže. Prednosti koje se mogu izdvojiti su fleksibilnost prilikom odabira rute usmjeravanja i brzina reakcije mreže na lokalizirane kvarove ili greške na pojedinom čvoru. Nedostatci su odabir ruta usmjeravanja koje nisu optimalne i potencijalni zastoji u prijenosu podataka zbog nedostatka informacija o stanju cijele mreže [21]. Odabir načina usmjeravanja između usmjeravanja temeljenog na podacima ili usmjeravanja temeljenog na adresi ovisi o vrsti aplikacije koja se koristi. U tradicionalnim mrežama podatkovni paketi se obično prosljeđuju na temelju adresa njihovih odredišnih čvorova. Primjer tome mogu biti video konferencije čiji su multimedijski paketi namijenjeni samo sudionicima u video pozivu tj. njihovim uređajima koji imaju jedinstvenu adresu. Ovakav način usmjeravanja naziva se usmjeravanje temeljeno na adresi.

Veliki dio IoT primjena zahtijeva protok svih ili većeg dijela generiranih informacija prema čvorovima koji obrađuju te informacije. Na primjer RFID čitač skenira sve RFID kartice unutar dometa ili senzorski čvorovi u WSN-u periodično šalju svoje podatke o određenom događaju prema WSN baznoj stanici. U takvim primjenama važno je da čvorovi s istim tipovima podataka ne šalju podatke prema određenoj adresi, već prema odredištu. Kako bi se spriječilo dupliranje informacija u čvorovima, stvaraju se tokovi podataka koji pružaju istu ili sličnu informaciju te se grupirani šalju na odredište. Takav način usmjeravanja naziva se usmjeravanje temeljeno na podacima, a ono je obično posljedica upita koji su poslani u mrežu od strane krajnjeg odredišta pomoću protokola usmjeravanja [21].

4.3.2. Usmjeravanje temeljeno na lokaciji i na stanju

Usmjeravanje temeljeno na lokaciji i usmjeravanje temeljeno na stanju se odnosi na vrstu informacija koje protokol usmjeravanja koristi za prosljeđivanje podatkovnih paketa. Protokol usmjeravanja koji se temelji na lokaciji, informacije o položaju čvorova koristi za adresiranje čvorova i prosljeđivanje podatkovnih paketa. Lokacije čvorova mogu se odrediti pomoću hardvera (npr. GPS senzor) ili pomoću softvera (npr. algoritmi određivanja lokacije). Prednosti usmjeravanja temeljenog na lokaciji su: niski troškovi održavanja i kontrole te skalabilnost i robusnost s obzirom na dinamičnost mreže. Informacije o mrežnoj topologiji za ovaj način usmjeravanja nisu potrebne, a procesi pronalaska i održavanja rute usmjeravanja su kratkotrajni. Nedostatak ovakvog načina usmjeravanja je ovisnost o mrežnim resursima pomoću kojih se određuje lokacija čvorova čiji su troškovi održavanja visoki.

Usmjeravanje temeljeno na stanju se odnosi na usmjeravanje koje ovisi o trenutnom stanju mreže. Stanje mreže može biti pohranjeno u čvorovima i/ili u podatkovnim paketima koji se prenose. Kada je stanje mreže pohranjeno u čvoru, svaki čvor ima pregled trenutne topologije mreže u smislu udaljenosti između čvorova i njihove povezanosti. U slučaju kada je stanje mreže pohranjeno u podatkovnim paketima, put usmjeravanja podatkovnog paketa od izvora do odredišta nalazi se u zaglavlju samog paketa. Glavni nedostatak usmjeravanja temeljenog na stanju je skalabilnost mreže, budući da je potrebna memorija za pohranu stanja mreže za svaki čvor. Također, stanje mreže može brzo zastarjeti ako se promjene topologije ne ažuriraju dovoljno često što uzrokuje pogrešno izračunate rute usmjeravanja [21].

4.3.3. Istorazinski i hijerarhijski načini usmjeravanja

Istorazinski i hijerarhijski načini usmjeravanja odnose se na pozicioniranje i izvršavanje algoritma usmjeravanja. U istorazinskom pristupu algoritam usmjeravanja je relativno jednostavan i primijenjen je na svakom čvoru u mreži. Čvor izvršava odluke o usmjeravanju

isključivo temeljene na informaciji o vlastitom stanju i stanju susjednih čvorova. S obzirom na jednostavnost dizajna i male zahtjeve za performansama uređaja, čak i mali IoT uređaji mogu biti čvorovi u mreži. Ovaj način usmjeravanja ne zahtijeva glavni čvor koji upravlja cijelom mrežom.

U hijerarhijskom načinu usmjeravanja čvorovi su podijeljeni na nekoliko hijerarhijskih razina. Pretpostavlja se da unutar svake razine svi uređaji imaju istu količinu resursa. Algoritam usmjeravanja se dijeli na komponente sa različitom razinom kompleksnosti, tako da je različitim razinama dodijeljen algoritam primjeren njihovim količinama resursa. Ovaj način usmjeravanja gdje su određene razine kompleksnosti i uloge svakog čvora u hijerarhiji, resursi mreže efikasnije se koriste za određivanje rute usmjeravanja [21].

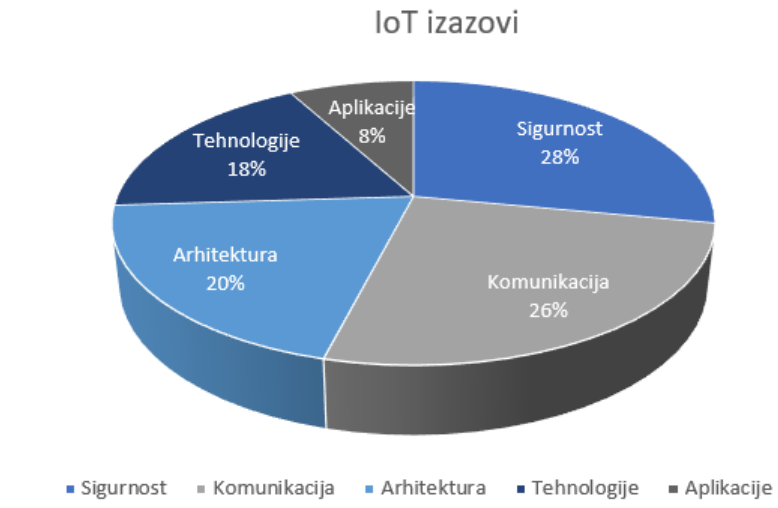
4.4. Moguća rješenja za IoT izazove

S velikim potencijalom IoT -a, pojavljuju se različite vrste izazova koje su navedene u poglavlju 4.1.. Sigurnost je jedno od glavnih pitanja IoT uređaja, tehnologija, aplikacija i platforme. IoT rješenju je potrebna učinkovita i funkcionalna sigurnost kako bi se osigurala anonimnost podataka, povjerljivost, integritet, autentifikacija, kontrola pristupa i sposobnost identifikacije, kao i heterogenost, skalabilnost i dostupnost te zbog toga nisu dopušteni sigurnosni propusti. IoT sigurnost mora omogućiti komunikacijsku privatnost, povjerljivost, dostupnost i integritet. Za zaštitu IoT komunikacije od prekida i neovlaštenog pristupa podacima koji se prenose, sigurnost se mora provoditi u svim slojevima arhitekture, od najnižeg do najvišeg sloja [26]. Postoji nekoliko metoda koje se mogu primijeniti kako bi se osigurala sigurnosti [8]:

- Svi IoT uređaji trebali bi se autentificirati provjerom softvera putem digitalnih potpisa, certifikata i drugih sigurnosnih metoda za sigurnu komunikaciju kroz mrežu.
- Osmišljena IoT sigurnosna rješenja moraju posjedovati pet ključnih funkcija kao što su: šifriranje podataka, mrežna sigurnost, identifikacija, korisnički pristup i upravljanje te analitika.

S povećanjem broja heterogenih uređaja u IoT dinamičkom okruženju, vrste ranjivosti se također povećavaju. Aplikacije i usluge moraju biti robusne i vrlo sigurne za pružanje pouzdanog upravljanja IoT-ovim skalabilnim umrežavanjem heterogenih pametnih uređaja. Općenito, kako bi se zaštitila privatnost podataka i spriječilo lažiranje i miješanje podataka, sustav ne smije ovisiti o drugim sustavima.

Potrebno je više rada na stvaranju rješenja za definirane izazove kako bi se mogle zadovoljiti globalne potrebe, osobito u područjima sigurnosti, tehnologije i komunikacija. Kao što je prikazano na slici 16, sigurnost i komunikacija postale su glavno područje rasprave o izazovima IoT-a jer je zahtjev za kvalitetom usluge u smislu privatnosti, sigurnosti i performansi na visokoj razini. Nekoliko izazova poput skalabilnosti, heterogenosti, dinamičnosti okruženja i interoperabilnosti imaju potencijal usporiti razvoj IoT-a. Kako bi se prepoznala korist IoT rješenja, aplikacije moraju biti neovisne, senzori moraju biti samoodrživi, arhitektura mora biti stabilna, a komunikacija mora biti sigurna [8].

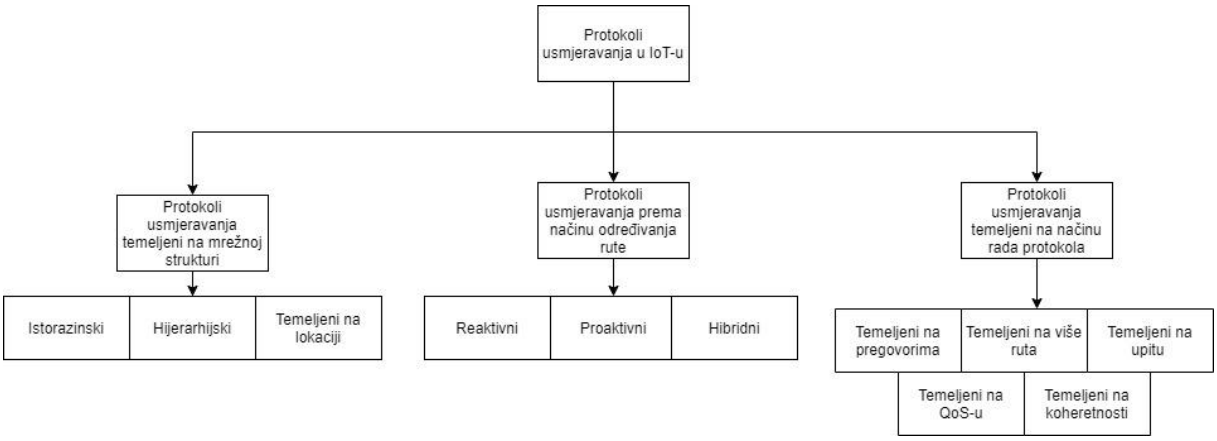


Slika 16. IoT izazovi

Izvor: [8]

5. Kategorizacija protokola usmjeravanja s obzirom na različite operativne zahtjeve

Usmjeravanje je proces odabira puta prijenosa informacija, a zadatak protokola usmjeravanja je pronalazak optimalnog i najkraćeg puta od izvora do odredišta. Kako bi se IoT mreža nosila s ograničenjima i izazovima koji su definirani u 4. poglavlju, protokoli usmjeravanja trebali bi biti dizajnirani na način na koji će zadovoljiti posebne zahtjeve i upotrijebiti različite strategije prilikom usmjeravanja. U svakom slučaju protokol mora odgovarati području primjene te biti „snalažljiv“ u smislu energetske potrošnje. Protokoli usmjeravanja mogu se kategorizirati s obzirom na različite operativne zahtjeve u tri kategorije, a to su: protokoli usmjeravanja temeljeni na mrežnoj strukturi, protokoli usmjeravanja prema načinu određivanja rute i protokoli usmjeravanja temeljeni na načinu rada protokola [27]. Navedena kategorizacija prikazana je na slici 17.



Slika 17. Kategorizacija protokola usmjeravanja u IoT mrežama

Izvor: [27]

5.1. Protokoli usmjeravanja temeljeni na mrežnoj strukturi

U IoT konceptu, mrežna organizacija ima važnu ulogu kod odabira protokola usmjeravanja, a ti protokoli koji se temelje na mrežnoj strukturi mogu biti [27]:

- istorazinski protokoli usmjeravanja
- hijerarhijski protokoli usmjeravanja
- protokoli usmjeravanja temeljeni na lokaciji.

Detaljniji opis istorazinskog, hijerarhijskog i usmjeravanja temeljenog na lokaciji definirani su u 4.3. poglavlju, kao i njihove prednosti i nedostatci, a u nastavku su navedene njihove osnovne karakteristike.

Istorazinski protokoli usmjeravanja primjenjuju se u mrežama koje imaju istorazinsku ili horizontalnu mrežnu strukturu, odnosno u mrežama gdje se svi čvorovi podjednako tretiraju. Istorazinske mreže karakterizira niska razina operativne složenosti i visoka učinkovitost što znači da u ovakvim mrežama nije potrebna organizacija mreže i mrežnog prometa, jer svi čvorovi imaju iste karakteristike i funkcionalnosti, a paketi se šalju između tih međusobno povezanih senzorskih čvorova.

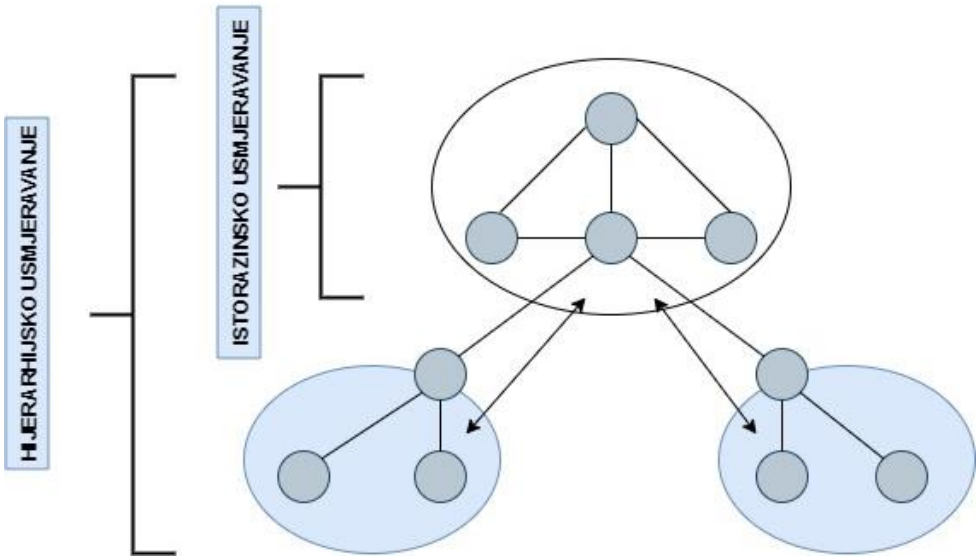
Protokoli koji se koriste u ovim mrežama su: SPIN (engl. *Sensor Protocol for Information via Negotiation*), DD (engl. *Directed Diffusion*), RR (engl. *Rumor Routing*) i MCFA *(*engl. *Minimum Cost Forwarding Algorithm*).

Hijerarhijski način usmjeravanja, odnosi se na mrežnu topologiju koja je podijeljena u hijerarhijske razine, poput klastera i glava klastera u odnosu na njihovu potrošnju energije. Cilj ovog usmjeravanja je smanjenje veličina tablica usmjeravanja. Grupe klastera se također nazivaju i domenama unutar kojih klasteri mogu komunicirati samo s onim klasterima koji su dio njihove domene, dok se komunikacija s ostalim klasterima odvija preko glave klastera koja je određena unutar svake domene tj. hijerarhije. Glave klastera su većinom usmjerivači s najboljim performansama. Razlika između istorazinskog i hijerarhijskog načina usmjeravanja vidljiva je na slici 18.

Najčešće korišteni protokoli koji se temelje na navedenim klasterima su: LEACH (engl. *Low Energy Adaptive Clustering Hierarchy*), PEGASIS (engl. *The power-efficient gathering in sensor information systems*), SOP (engl. *Self Organizing Protocol*), TEEN (engl. *Threshold sensitive Energy Efficient sensor Network protocol)*, APTEEN (engl. *Adaptive Threshold-sensitive Energy Efficient Network*), VGA (engl. *Virtual Grid Architecture*).

Usmjeravanje temeljeno na lokaciji je vrsta usmjeravanja gdje se određuje lokacija senzorskih čvorova na temelju snage signala čvora, a lokacija susjednih čvorova se uglavnom dobiva tako što se šalju paketi o lokaciji kroz sve slojeve mreže. Procedure uspostave i održavanja rute nisu uključene u ovu vrstu usmjeravanja, a podatkovni paketi šalju se između susjednih čvorova sve dok ne pristignu do ciljanog čvora čija je lokacija poznata. Senzori koji posjeduju veću energetsku snagu koriste se za obradu i prosljeđivanje paketa, dok oni s nižom energetskom razinom služe samo za slanje i primanje tih paketa.

Protokoli koji se najčešće koriste za ovakvu vrstu usmjeravanja su: GAF (*engl. Geographic Adaptive Fidelity*), LPBR (*engl. Location Prediction Based Routing Protocol*), SPAN (*engl. Switch Port Analyzer*) te GOAFR (*engl. Greedy Other Adoptive Face Routing*).



Slika 18. Istorazinski i hijerarhijski način usmjeravanja

Izvor: [28]

5.2. Protokoli usmjeravanja prema načinu određivanja rute

Usmjeravanje prema načinu određivanja rute predstavlja održavanje rute od izvora do odredišta kojom se prenose informacije. Navedeni protokoli usmjeravanja klasificirani su na načina na koji donose odluke o usmjeravanju [27]:

- proaktivni protokoli usmjeravanja
- reaktivni protokoli usmjeravanja
- hibridni protokoli usmjeravanja.

Reaktivni protokoli usmjeravanja ne posjeduju informacije o susjednim čvorovima i rutama za usmjeravanje, zbog toga se često koriste u dinamičkim mrežama koje podržavaju stalne promjene u topologiji. Navedeni protokoli funkcioniraju „na zahtjev“ (*engl. on-demand*), odnosno zahtijevaju rutu za usmjeravanje samo kad postoji potreba za slanjem podataka kroz mrežu. Reaktivni protokoli usmjeravanja primjenjivi su u mrežama s manjim prometom, jer potreba za traženjem rute prije prijenosa korisničkih podataka povećava kašnjenje u tom prijenosu.

Najčešće korišteni reaktivni protokoli usmjeravanja su: AODV (engl. *Ad-hoc on-demand distance vector routing system*), DSR (engl. *Dynamic source routing*), TORA (engl. *Temporarily ordered routing algorithm*) i SEER (engl. *Spectrum and Energy Efficient routing protocol*).

Proaktivni protokoli usmjeravanja za razliku od reaktivnih protokola uglavnom se koriste u mrežama statične topologije. Proaktivni protokoli mogu se nazivati još i protokoli vođeni tablicom jer postupak usmjeravanja izvršavaju na temelju tablice usmjeravanja, a njihova prednost je to što su u mogućnosti kontinuirano obnavljati tu tablicu usmjeravanja te na taj način svi čvorovi u mreži uglavnom posjeduju ispravnu sliku mrežne topologije.
Proaktivni protokoli usmjeravanja koji se uglavnom koriste su: OLSR (engl. *Optimized linked state routing*), DSDV (engl. *Destination sequenced distance vector*), TBRPF (engl. *Topology dissemination based on reverse path forwarding*) i GPSR (engl. *Greedy Perimeter Stateless Routing*).

Hibridni protokoli usmjeravanja smatraju se kombinacijom reaktivnih i proaktivnih protokola usmjeravanja jer sadrži karakteristike i funkcionalnosti navedenih vrsta protokola. Hibridni protokoli prilikom komunikacije s određenim dijelovima mreže koriste reaktivno usmjeravanje, a s ostalim dijelovima proaktivno usmjeravanje. Ponekada, određene situacije u komunikaciji i usmjeravanju nisu jasno određene, pa se kombinacijom funkcionalnosti reaktivnih i proaktivnih protokola usmjeravanja može postići veća učinkovitost i efikasnost prilikom usmjeravanja.
Primjenjivi hibridni protokoli usmjeravanja su: ZRP (engl. *Zone based routing protocol*) i SOC-M2M (engl. *Self-Organized Clustering Machine-to-Machine*).

5.3. Protokoli usmjeravanja temeljeni na načinu rada protokola

Protokoli usmjeravanja koji se temelje na načinu rada su protokoli koji imaju različite operativne zahtjeve i karakteristike, a ti protokoli kategorizirani su na sljedeći način [27]:

- protokoli usmjeravanja temeljeni na pregovorima
- protokoli usmjeravanja temeljeni na više ruta
- protokoli usmjeravanja temeljeni na upitu
- protokoli usmjeravanja temeljeni na QoS-u (engl. *Quality of Sevice*)
- protokoli temeljeni na koherentnosti.

Protokoli usmjeravanja temeljeni na pregovorima koriste se u usmjeravanju koje će ukloniti suvišne podatke nastale između izvora i odredišta. Zbog uspješnije izvedbe procesa usmjeravanja, uštede energije i duljeg vijeka trajanja mreže proces pregovora tj. uklanjanja suvišnih podataka izvršava se neposredno prije početka usmjeravanja, a temelju dostupnosti resursa donijet će se pregovaračke odluke.

Protokoli usmjeravanja temeljeni na više ruta služe za organiziranje neometane komunikacije, uravnoteženje opterećenja, a također i za poboljšanje kvalitete usluge. Navedeni protokoli posjeduju mehanizam tolerancije grešaka te su zbog toga u mogućnosti konstruirati veliki broj ruta, također se za svaku rutu provjeravaju energetski zahtjevi za periodično slanje podataka. Izazovi koje je teško postići su pouzdanost, maksimalni vijek trajanja mreže i smanjenje kašnjenja. Kako bi se smanjilo zagušenja mreže i maksimizirale performanse mreže u protokolima usmjeravanja koristi se više ruta za prijenos podataka. Kada se koristi više ruta postoji mogućnost korištenja alternativnih puteva za dolazak do odredišta. Protokoli koji se koriste za usmjeravanje temeljeno na više ruta mogu biti: AOMDV (engl. *Ad-hoc on demand Multipath Distance Vector*), DSDV (engl. *Destination Sequence Distance Vector*), HEED (engl. *Hybrid Energy Efficient Distributed Clustering*), LEACH (engl. *Low Energy Adaptive Clustering Hierarchy*) i GEAR (engl. *Geographic and Energy Aware Routing*).

Protokoli usmjeravanja temeljeni na upitu usmjeravanje izvršavaju razmjenom podataka pomoću upita i odgovora. Prijemni čvorovi šalju poruku zahtjeva po cijeloj mreži i samo oni čvorovi koji imaju potreban odgovor na podatke, odgovaraju na taj zahtjev.

Protokoli usmjeravanja temeljeni na QoS-u koriste se u mrežama koje moraju regulirati potrošnju energije i QoS. Točnije, kad god odredište zahtijeva podatke od čvora u mreži, prijenos mora zadovoljiti određenu razinu QoS kao što su kašnjenje i propusnost, pri isporuci podataka baznoj stanici. Na temelju QoS-a usmjeravanje se obično postiže rezervacijom resursa u povezanoj komunikaciji koja zadovoljava QoS zahtjeve za svaku rutu. Najvažniji protokoli ovih karakteristika su RPL (engl. *Routing Protocol for Low-Power and Lossy Networks*) i SAR (engl. *Sequential assignment routing*).

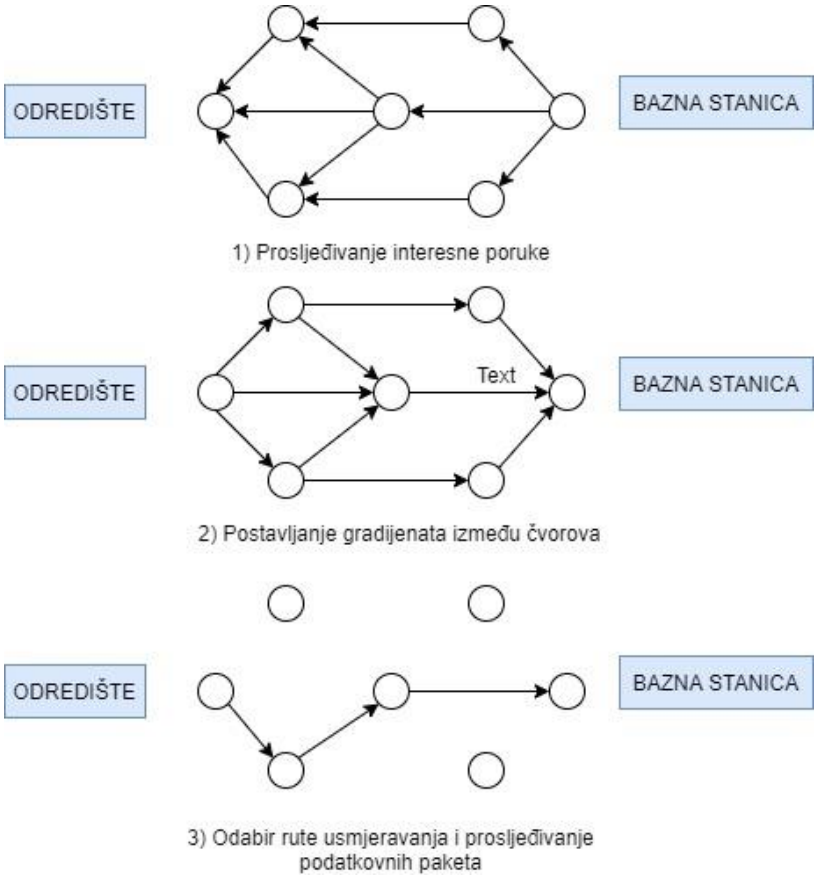
Koherentni i nekoherentni protokoli odnose se na protokole usmjeravanja koji se temelje na obradi podataka. Koherentni protokoli usmjeravanja zaduženi su za dodavanje vremenske oznake podacima te za uklanjanje nepotrebnih i duplih podataka. Nekoherentni protokoli usmjeravanja zaduženi su samo za obradu sirovih podataka nakon čega podatke prosljeđuju drugim čvorovima koji su zaduženi za daljnju obradu [27].

6. Analiza performansi protokola primjenjivih za IoT mreže

Protokoli koji su primjenjivi u IoT mrežama, mogu se kategorizirati s obzirom na različite operativne zahtjeve, kao što je prikazano u 5. poglavlju. Svaki pojedini protokol ima svoje karakteristike, funkcionalnosti i razloge primjene. Većina protokola WSN mreže implementirani su i primjenjivi u IoT mrežama s minimalnim poboljšanjem istih (npr. s obzirom na energetsku potrošnju, propusnost i sl.). Energija je oskudan resurs u IoT mreži, stoga očuvanje energije predstavlja značajan izazov ove mreže. Smanjenje te potrošnje može se postići na nekoliko načina, od kojih je jedan odabir optimalne rute za prijenos podataka. Navedeno se postiže odabirom adekvatnih protokola usmjeravanja. U nastavku su definirani značajniji protokoli usmjeravanja u IoT mrežama s obzirom na različite parametre i performanse.

6.1. DD i RR protokoli

DD odnosno protokol izravne difuzije pripada skupini istorazinskih protokola usmjeravanja koji je orijentiran na podatke, a njegov pristup usmjeren na podatke te uklanja potrebu za adresiranjem čvorova. Podatke koje DD protokol prikuplja od strane različitih čvorova nazivaju se atributnim vrijednostima. DD protokol sastoji se od interesne poruke, podatkovne poruke, gradijenta i selekcija. Interesne poruke sastoje se od atributnih vrijednosti koje opisuju zadatak koji je potrebno izvršiti. Gradijent određuje brzinu prijenosa podataka, kao i smjer događaja, a selekcija odabire određenu rutu usmjeravanja. U istorazinskom protokolu podaci koji dolaze iz različitih izvora kombiniraju se i na taj se način uklanjaju suvišni podaci. Shodno tome, smanjuje se broj prijenosa, štedeći mrežnu energiju i produljujući njezin vijek trajanja. Prilikom izravne difuzije, bazna stanica raspršuje upit prema čvorovima u području od interesa. Svaki čvor prima interesne poruke i postavlja gradijent prema čvorovima od kojih prima tu interesnu poruku, a gradijent se može zamisliti kao povratna veza između čvorova. Navedeni proces rada DD protokola prikazan je na slici 19. Posrednički čvorovi zaduženi su za agregaciju podataka, odnosno uklanjanje nepotrebnih i dupliciranih podataka, čime se smanjuju troškovi komunikacije. Čvor zatim šalje opis događaja svakom susjednom čvoru za koji ima gradijent, a susjedni čvor koji prima te podatke traži podudaranje primljenih podataka u svojoj predmemoriji. Ako se pronađe podudaranje podataka, čvor prosljeđuje podatkovnu poruku bez daljnjih radnji, no ako podudaranje ne postoji čvor dodaje poruku u svoju predmemoriju, zatim je prosljeđuje do susjednih čvorova [29].



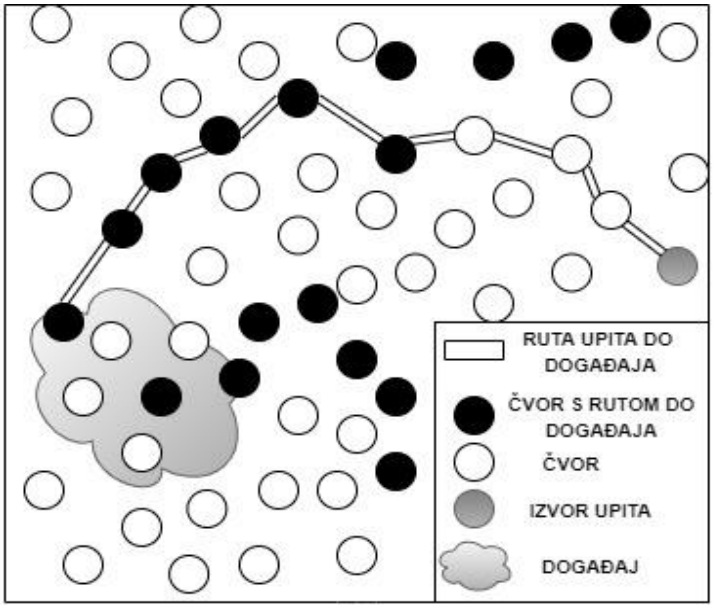
Slika 19. Način rada DD protokola

Izvor: [21]

RR protokol usmjeravanja je vrsta direktne difuzije i koristi se za aplikacije u kojima geografsko usmjeravanje nije izvedivo. Kombinira protokole poplava upita i poplava događaja na slučajan način. RR protokol svoj način rada usmjerava na temelju pretpostavki da se mreža sastoji od gusto raspoređenih čvorova, da su dopušteni samo prijenosi podataka na kratke udaljenosti te da mreža posjeduje fiksnu infrastrukturu.

U slučaju direktne difuzije poplava se koristi za prosljeđivanje upita po cijeloj mreži. Ponekad je traženi broj podataka iz čvorova minimalan, pa je algoritam poplave nepotreban, zbog toga se upotrebljava drugi pristup koji se odnosi na algoritam preplavljivanja događaja, tj. kada je broj događaja minimalan, a broj upita velik. Upiti su pohranjeni u određene čvorove koji pripadaju interesnoj skupini. Kako bi preplavio događaje kroz mrežu, RR protokol koristi dugotrajne pakete, nazvane agentima. Kada čvor detektira događaj, dodaje takav događaj u svoju tablicu događaja i generira agenta. Agenti putuju mrežom slučajnim putem sa srodnim informacijama o događaju te tada posjećeni čvorovi tvore gradijent prema događaju. Kad čvor treba pokrenuti upit, usmjerava upit prema početnom izvoru. Za razliku od direktne difuzije, odnosno DD protokola usmjeravanja, gdje se podaci mogu usmjeravati kroz više postavljenih

ruta usmjeravanja po definiranim brzinama, usmjeravanje pomoću RR protokola održava samo jedan put između izvora i odredišta, kao što je prikazano na slici 20. Navedeni način rada RR protokola funkcionira samo kada je nizak broj događaja u mreži, dok suprotno tome tj. veći broj događaja u mreži povećava i troškove održavanja agenata i tablica događaja u svakom čvoru [29].



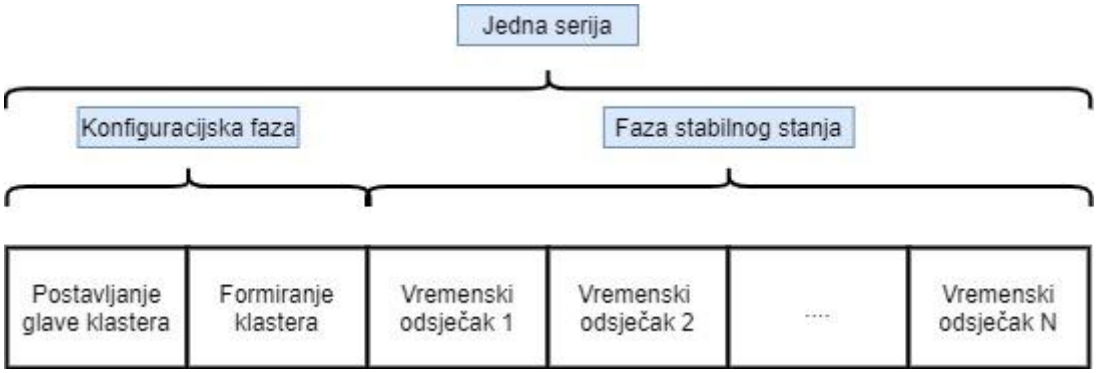
Slika 20. Način rada RR protokola usmjeravanja
Izvor: [30]

6.2. LEACH i PEGASIS protokoli

Prvi protokol dizajniran za dinamičko usmjeravanje, a koji pripada grupi hijerarhijskih protokola usmjeravanja je LEACH. U mreži u kojoj se koristi navedeni protokol, klasteri su pozicionirani slučajnim načinom na temelju hijerarhijskog modela usmjeravanja, gdje se od svih postavljenih klastera unutar svake grupe tj. hijerarhije bira glava klastera koja ima ulogu prikupljanja podataka od svih pridruženih čvorova u hijerarhiji. Glavna odgovornost glave klastera je prenošenje podataka i informacija unutar vlastite grupe klastera, do druge grupe klastera ili do bazne stanice. Nedostatak protokola koji se temelje na klasterima je vrijeme utrošeno na odabir glave klastera unutar skupine klastera [27].

LEACH protokol karakterizira niska energetska potrošnja te odgovornost za produživanje vijeka trajanja same mreže. Navedeni protokol se sastoji od dva segmenta, što je prikazano i na slici 21, gdje se prvi segment naziva konfiguracijska faza i odnosi na formiranje klastera i odabir glave klastera. Drugi segment naziva se stacionarna faza tj. faza stabilnog stanja koja

predstavlja mjesto gdje se odvija stvarni prijenos podataka i informacija. Mobilni senzori koriste se za obradu i prijenos podataka [31].

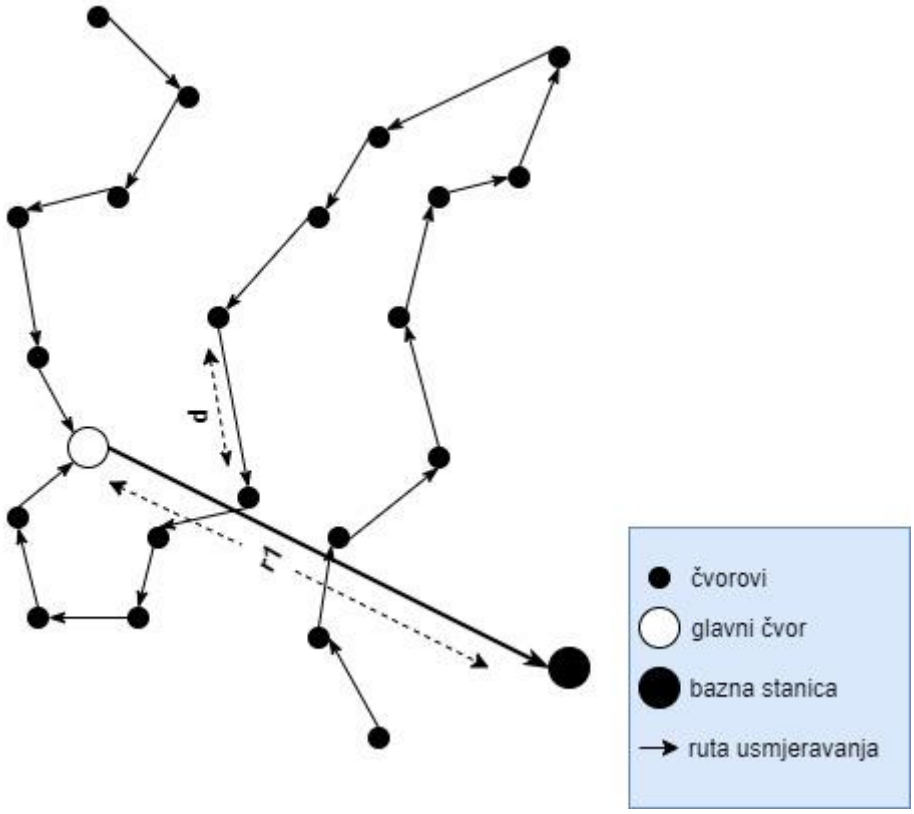


Slika 21. Faze LEACH protokola usmjeravanja

Izvor: [32]

Nadalje, protokol PEGASIS se smatra modificiranom verzijom LEACH protokola i također pripada skupini hijerarhijskih protokola usmjeravanja. Za razliku od LEACH-a, kod primjene PEGASIS protokola svi čvorovi u mreži mogu međusobno komunicirati, odnosno slati i primati podatke te svi posjeduju sveobuhvatne informacije o cijeloj mreži senzora. Temeljni koncept PEGASIS-a razlikuje se od drugih hijerarhijskih protokola usmjeravanja jer se ne temelji na klasterima, nego na strukturi lanca. Za razliku od LEACH protokola koji se definira kroz dvije faze, PEGASIS protokol sastoji se od tri faze rada koje uključuju izgradnju lanca, odabir vođe čvorova i prijenos podataka. Struktura lanca prikazana je na slici 22, a gradi se na temelju svakog čvora koji ima potrebne informacije o svom susjednom čvoru te ga na taj način dodaje u lanac. Vođa lanca tj. prvi čvor preuzima odgovornost prijenosa podataka do bazne stanice, pri čemu svaki čvor mijenja svoju ulogu vođe što omogućuje uravnoteženu raspodjelu energetskog opterećenja među čvorovima, a samim time je uravnotežena i regulirana potrošnja energije po svakom novom usmjeravanju. Tijekom prikupljanja podataka u PEGASIS-u, osim vođe čvorova lanca, svaki drugi čvor spaja svoje podatke zajedno s primljenim podacima od svog najbližeg susjeda kako bi proizveo jedan paket podataka identične duljine i proslijedio ih sljedećem susjedu duž lanca.

Osnovna svrha predloženog rješenja je smanjenje brzine prijema paketa između glave klastera i čvorova, što može dovesti do poboljšanog vijeka trajanja mreže te kao što je već navedeno, uravnotežene potrošnje energije unutar cijele mreže. Međutim, izgrađene rute nisu optimalne, zbog čega zahtijevaju dodatne troškove i prijelome ruta usmjeravanja [33].



Slika 22. Način usmjeravanja pomoću PEGASIS protokola

Izvor: [34]

Na temelju slike i detaljnog opisa PEGASIS protokola, mogu se pretpostaviti i navesti razni nedostatci ovog protokola [35]:

- Teško je postići pretpostavku da svi čvorovi imaju potrebno znanje o svim čvorovima u mreži, dok duga lančana struktura može uzrokovati veliko kašnjenje prilikom prijenosa, što povezuje problem skalabilnosti.
- Odabir vođe lanca izvršava se bez razmatranja informacija o svim čvorovima u mreži. Također, izabrani vođa tj. glavni čvor trebao bi biti sposoban izravno komunicirati s baznom stanicom.
- Ne postoje posebni kriteriji za identifikaciju najudaljenijeg čvora u mreži. Stoga će vođe čvorova smješteni na udaljenim pozicijama od bazne stanice trošiti visoku energiju za prijenos podataka do bazne stanice, dok čvorovi koji su bliže pozicionirani baznoj stanici neće moći izvršiti taj prijenos.
- Vođa čvorova koji se nalazi u slučajnoj točki mreže može dovesti do velikog kašnjenja prilikom prijenosa s kraja na kraj.

6.3. TEEN i APTEEN protokoli

S obzirom na mrežnu strukturu TEEN i APTEEN protokoli pripadaju hijerarhijskim protokolima usmjeravanja, što je vidljivo na slici 23, no s obzirom na način odabira rute za prijenosa podataka TEEN se smatra reaktivnim protokolom, a APTEEN hibridnim protokolom usmjeravanja.

TEEN je prvi protokol koji je razvijen za svrhe reaktivnog načina usmjeravanja. S obzirom na formiranje mreže klastera može se poistovjetiti sa LEACH protokolom. Glavne značajke ovog protokola su sljedeće:

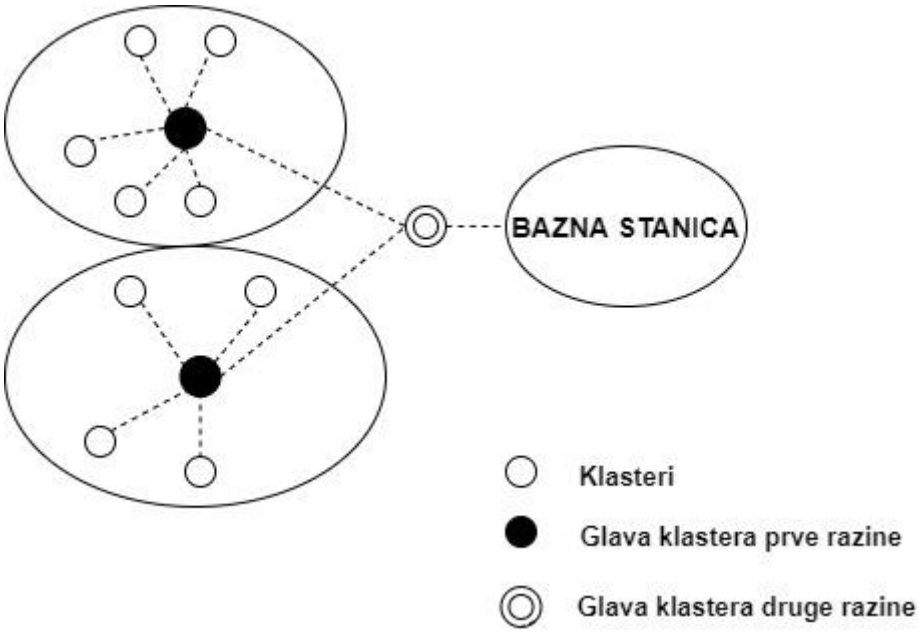
- Vremenski kritični podaci dopiru do korisnika u stvarnom vremenu, što znači da je ovaj protokol izrazito prikladan za aplikacije koje služe za mjerenje vremenski kritičnih podataka.
- Prijenos poruka troši puno više energije nego otkrivanje samih podataka, ali potrošnja energije pomoću ovog protokola potencijalno može biti puno manja nego u proaktivnoj mreže, jer se prijenos podataka obavlja rjeđe.
- Osjetljivi podaci, ovisno o kritičnosti osjetnog atributa i ciljane aplikacije, mogu dati točniju sliku mreže, na račun povećane potrošnje energije. Tako korisnik može kontrolirati kompromis između energetske učinkovitosti i točnosti podataka.
- U svakom trenutku promjene klastera, atributi se emitiraju iznova, pa ih korisnik može promijeniti prema potrebi.

Glavni nedostatak ove sheme je da, ako se podaci ne prikupe, čvorovi nikada neće komunicirati, a korisnik neće dobiti nikakve podatke s mreže i neće saznati čak ni ako svi čvorovi prestanu funkcionirati. Shodno tome, navedeni protokol nije dobro prilagođen aplikacijama pomoću kojih korisnik mora redovno dobivati podatke. Također je potrebno izbjeći interakciju i sudare između klastera, a navedeno je moguće pomoću TDMA (engl. *Time-division multiple access*) raspoređivanja čvorova za izbjegavanje navedenog problema. To će, međutim, uvesti kašnjenje u izvještavanju kada su u pitanju važni podaci, pa se zbog toga često koristi CDMA (engl. *Code-division multiple access*) kao rješenje [36].

Zbog navedenih nekoliko nedostataka, razvijena poboljšana verzija protokola TEEN je APTEEN koji je za razliku od TEEN-a razvijen za hibridne mreže, no njihova hijerarhijska struktura usmjeravanja je ista te je prikazana na slici 23. Prema [27], u APTEEN-u, glave klastera proizvodi različite vrste parametara:

- Proizvodi atribute koji su skupovi fizičkih parametara pomoću kojih korisnik dobiva potrebne podatke.
- Zatim, proizvodi podatke koji mogu biti manje ili više osjetljivi s obzirom na različite utjecaje.
- Navedeni protokol u mogućnosti je definirati i određene vremenske rasporede koji se postižu pomoću TDMA te se dodjeljuje svakom pojedinom čvoru.
- APTEEN također definira maksimalno dopušteno vremensko razdoblje unutar kojeg podaci poslani od čvora trebaju stići na odredište.

APTEEN omogućuje korisniku postavljanje graničnih vrijednosti, kao i odbrojavanje vremenskog intervala, što znači ako čvor ne šalje podatke u vremenskom razdoblju jednakom vremenu odbrojavanja, prisiljen je ponovno poslati podatke, čime se održava potrošnja energije. Budući da je APTEEN hibridni protokol, može oponašati proaktivnu mrežu ili reaktivnu mrežu ovisno o vremenu odbrojavanja i vrijednosti podataka. Nedostatak ovog protokola je potrebna dodatna složenost za implementaciju zbog glave klastera koja proizvodi različite vrste parametre.

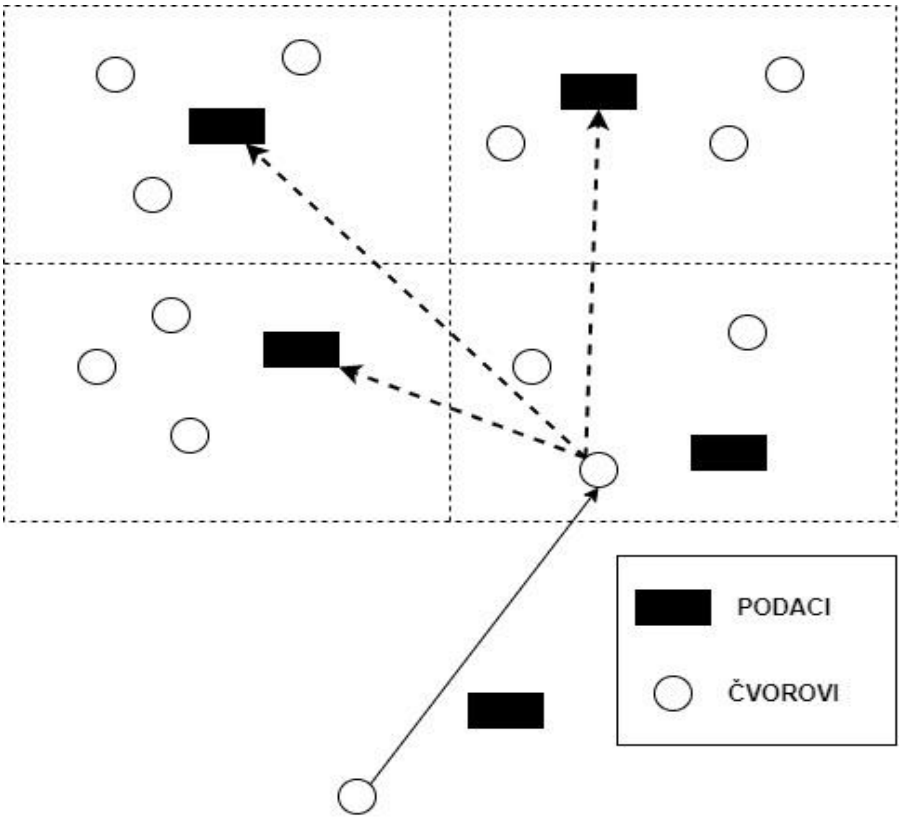


Slika 23. Hijerarhijska struktura kod TEEN i APTEEN protokola
Izvor: [29]

6.4. GEAR I GAF protokoli

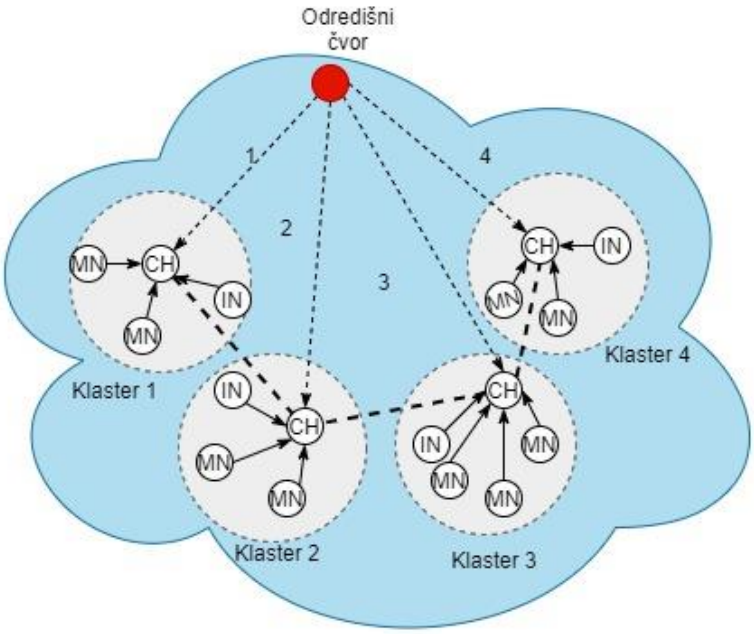
Protokoli usmjeravanja temeljeni na lokaciji za IoT mreže zahtijevaju informacije o lokaciji svih čvorova, koje su im potrebne za izračunavanje udaljenosti između bilo koja dva čvora u mreži. GEAR je protokol usmjeravanja koji se temelji na lokaciji i koji koristi GIS (Geografski informacijski sustav) za pronalaženje lokacije čvorova u mreži. Prema ovom protokolu, svaki čvor proizvodi dvije vrste troškova prilikom dolaska do odredišta: procijenjene troškove i stvarne troškove. Procijenjeni trošak podrazumijeva neutrošenu energije i udaljenosti do odredišta, dok se stvarnim troškom smatra definirani procijenjeni trošak i rupe u mreži koje nastaju kada čvor nema kome proslijediti podatke do ciljanog odredišta. U slučaju da nema rupa, procijenjeni trošak jednak je stvarnom trošku. GEAR protokol razmatra samo određeni dio mreže, ne šalje interesne poruke cijeloj mreži, za razliku od DD protokola usmjeravanja te na taj način štedi energetske resurse. Navedeni protokol svoj rad može podijeliti u dvije faze [29]:

- U prvoj fazi paketi se prosljeđuju prema ciljnom području. Nakon što je zaprimio paket, čvor traži susjeda koji je bliže ciljanom području, što znači da je odabrani susjedni čvor definiran kao sljedeći skok. Ako postoji više prikladnih čvorova odabire se jedan čvor za prosljeđivanje paketa na temelju stvarnih troškova. Na preostalim čvorovima koji nisu odabrani kao sljedeći skok će nastati rupa.
- U drugoj fazi paketi se prosljeđuju unutar ciljane regije. Ako paket dosegne ciljano područje, on se u tom području raspršuje rekurzivnim geografskim prosljeđivanjem ili ograničenim poplavama. Ako senzori nisu gusto raspoređeni, tada se koristi ograničeno preplavljivanje, a ako je gustoća čvora velika, tada se koristi geografsko preplavljivanje. U geografskim preplavljivanjima regija je podijeljena na četiri podregije kao što je prikazano na slici 24 i stvorene su četiri kopije paketa. Taj se proces nastavlja sve dok ne ostanu regije sa samo jednim pripadajućim čvorom.



Slika 24. Način rada GEAR protokola
Izvor: [37]

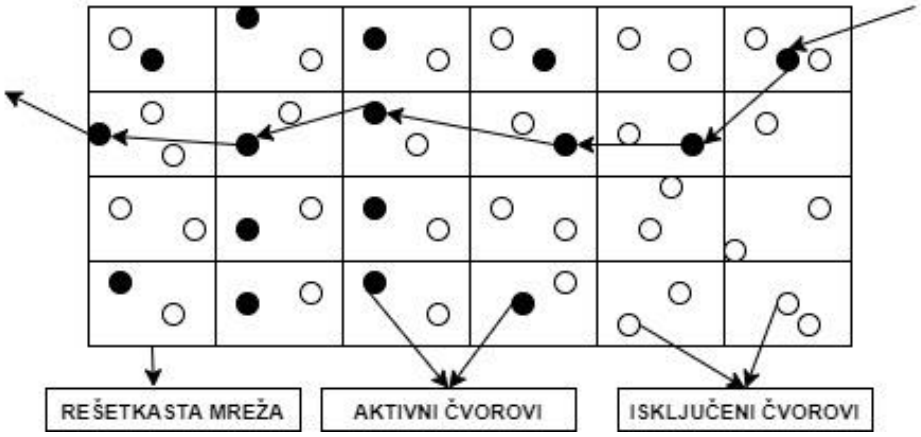
GEAR protokol koristi IN (engl. *Inspecting Nodes*) mehanizam temeljen na strategiji praćenja paketa kako bi se spriječilo namjerno uništavanje ili zlonamjerni napadi na prenošene podatke. Navedeni mehanizam posjeduje tri vrste čvorova, tj. glavne čvorove, IN čvorove i mobilne čvorove. Kao što je prikazano na slici 25, mogu se međusobno nadzirati i provjeravati. Nakon što IN čvor otkrije neke neobične radnje glavnog čvora, detektirani čvor stavit će na crnu listu i obavijestiti okolne mobilne čvorove da obustave prijenos podataka prema glavnom čvoru [38].



Slika 25. Topologija IN mehanizma
Izvor: [38]

Zatim, GAF protokol također pripada skupini protokola temeljenih na lokaciji, a s obzirom na svoju energetsku učinkovitost primjenjiv je u IoT mrežama. GAF se može implementirati i za nepokretne i za mobilne čvorove. Iako je GAF protokol temeljen na lokaciji, može se implementirati i kao hijerarhijski protokol gdje se klasteri temelje na geografskom položaju. U početku se područje interesa dijeli na neke fiksne zone koje tvore rešetkastu virtualnu mrežu za pokriveno područje, što je prikazano na slici 26. Čvorovi u svakoj zoni imaju različite funkcionalnosti i svaki čvor koristi svoju lokaciju označenu GPS-om kako bi se povezao s točkom u mreži. Čvorovi koji su postavljeni na istoj točki mreže smatraju se ekvivalentnima u smislu cijene usmjeravanja paketa. Takva se ekvivalentnost koristi za održavanje čvorova smještenih u određenom području mreže u stanju mirovanja zbog uštede energije. Stoga GAF može povećati životni vijek mreže s povećanjem broja čvorova. GAF štedi energiju isključivanjem nepotrebnih čvorova u mreži bez utjecaja na razinu vjernosti usmjeravanja. GAF definira tri stanja: aktivno stanje, isključeno tj. stanje mirovanja i stanje otkrivanja. Stanje otkrivanja koristi se za određivanje susjednog čvora u mreži, dok aktivno stanje sudjeluje u procesu usmjeravanja, a u vrijeme stanja mirovanja čvorovi isključuju svoju aktivnost. Kako bi upravljao mobilnošću, svaki čvor u mreži procjenjuje vrijeme napuštanja mreže i šalje to svojim susjednim čvorovima. Susjedni čvorovi koji su u stanju mirovanja u skladu s tim prilagođavaju vrijeme mirovanja kako bi zadržali vjernost rute. Prije nego što istekne vrijeme napuštanja

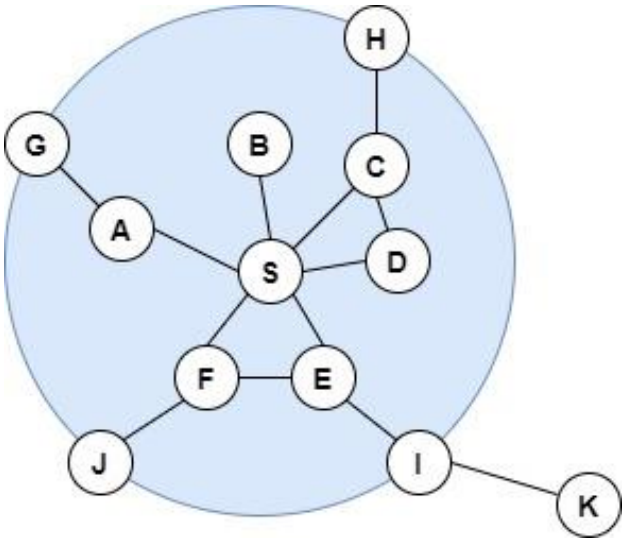
aktivnog čvora, čvorovi koji su isključeni se aktiviraju te se na taj način održava uspješno usmjeravanje podataka [29].



Slika 26. Način rada GAF protokola
Izvor: [39]

6.5. ZRP protokol

Proaktivno usmjeravanje koristi višak propusnosti za održavati informacije o usmjeravanju, dok reaktivno usmjeravanje uključuje duga kašnjenja zbog potrebe za zahtijevanjem rute. Cilj ZRP protokola je rješavanje navedenih nedostataka kombinirajući najbolja svojstva oba pristupa. Način rada ZRP protokola je prilagodljivo, a navedeno ponašanje ovisi o trenutnoj konfiguraciji mreže i zahtjevima korisnika. ZRP protokol, kako mu sam naziv govori, temelji se na konceptu zona. Zona usmjeravanja definirana je za svaki čvor zasebno, dok se zone susjednih čvorova preklapaju. Polumjer ρ izražen je u zoni usmjeravanja pomoću skokova. Zona tako uključuje čvorove, čija udaljenost od najdaljeg čvora može biti najviše ρ skokova. Jedan primjer zone usmjeravanja prikazan je na slici 27, gdje je zona usmjeravanja S te uključuje čvorove od A do I, ali ne i K. Na slici 27, polumjer je označen kao krug oko pripadajućih čvorova. Bitno je napomenuti kako je zona strukturirana u skokovima, a ne u fizičkoj udaljenosti [40].



Slika 27. Primjer usmjeravanja u zoni sa ρ=2
Izvor: [40]

Čvorovi zone podijeljeni su na periferne i unutarnje čvorove. Periferni čvorovi su čvorovi čija minimalna udaljenost do središnjeg čvora iznosi točno definiran polumjer zone ρ. Čvorovi čija je minimalna udaljenost manja od ρ su unutarnji čvorovi. Na slici 27 čvorovi A – F su unutarnji čvorovi, čvorovi G – J su periferni čvorovi a čvor K je izvan zone usmjeravanja. Primjenom ovog protokola usmjeravanja čvor H do središnjeg čvora može doći dvjema rutama, jednom duljine dva skoka, a drugom s duljinom od tri skoka. Broj čvorova u zoni usmjeravanja može biti reguliran pomoću prijenosne snage čvorova, što znači da smanjivanjem snage se smanjuje i broj čvorova u zoni. Broj susjednih čvorova trebao bi biti dovoljan za pružanje odgovarajuće dostupnost i redundantnost unutar zone usmjeravanja.

Ključna ideja ZRP protokola usmjeravanja je korištenje značajki proaktivnih i reaktivnih protokola usmjeravanje. Shodno tome, proaktivnim usmjeravanjem unutar ograničene zone, vrijeme uspostave veze može se smanjiti, dok se reaktivnim usmjeravanjem smanjuje potreba za kontrolom prometa pomoću otkrivanja ruta usmjeravanja na zahtjev za odredišta izvan zone usmjeravanja. ZRP protokol visoko je primjenjiv u IoT mrežama zbog mogućnosti prilagodbe velikim mrežama. Nadalje, novi protokoli koji nisu proaktivni ni reaktivni, nego protokoli koji koriste zemljopisne informacije su jedini koji mogu nadmašiti ZRP protokol [40].

6.6. RPL protokol

RPL pripada skupini protokola koji se temelje na načinu rada protokola, odnosno u ovom slučaju usmjeravanje izvršava na temelju QoS zahtjeva. IETF (engl. *The Internet Engineering Task Force*) je 2008. godine predstavio RPL protokol usmjeravanja za male mreže i mreže s

gubitcima. Misija IETF radne grupe bila je osmisliti protokol usmjeravanja koji bi mogao biti pogodan za mreže sastavljene od velikog broja ugrađenih uređaja s ograničenom snagom, memorijom i resursima za obradu podataka. Također, navedeni protokol bi trebao biti u stanju zadovoljiti zahtjeve širokog spektra korištenih aplikacija, kao npr. aplikacije za nadzor i upravljanje, poput automatizacije zgrada, industrijskog okoliša, zdravstva, prometa i sl. Ishod navedenih karakteristika i aktivnosti je RPL protokol usmjeravanja, standardiziran u ožujku 2012. godine. U nastavku su prikazana načela dizajna, najvažniji mehanizmi i značajke RPL protokola, kao i njegove prednosti i nedostatci.

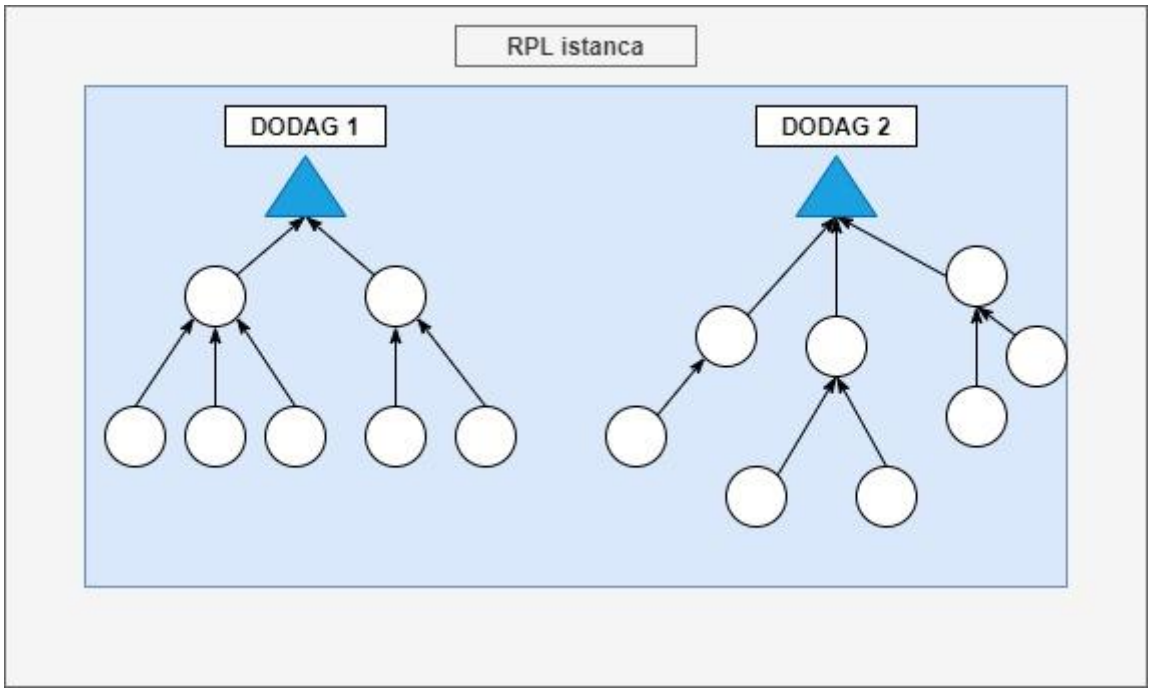
Načela dizajna RPL protokola usmjeravanja izravno proizlaze iz vrste mreža i prometa za koje je potrebno primijeniti RPL. Točnije, RPL je dizajniran za velike mreže koje se sastoje od velikog broja uređaja koji komuniciraju putem komunikacijskih tehnologija male snage i niske cijene. Iz tih razloga, glavni ciljevi RPL-a su:

- Smanjiti zahtjeve memorije (tj. skladišni prostor za održavanje usmjeravanja informacije i tablice usmjeravanja).
- Usvojiti mehanizme usmjeravanja i prosljeđivanja podataka niske složenosti kako bi se olakšala implementacija na jednostavnim mikrokontrolerima s ograničenim sposobnostima.
- Smanjiti troškove signalizacije usmjeravanja te smanjiti potrošnju propusnosti i energetsku potrošnju.
- Također, jedan od ciljeva je i učinkovito otkrivanje ruta usmjeravanja za mreže koje nemaju unaprijed definiranu topologiju.

Nadalje, RPL se uglavnom upotrebljava za zahtjeve usmjeravanja u mrežama koje služe za prikupljanje podataka, gdje je većina prometa usmjerena od više točaka prema jednoj točki, odnosno teče iz RPL čvorova prema jednoj točki okupljanja mreže. S druge strane, RPL je manje učinkovit prilikom usmjeravanja podataka od točke prema više točaka, odnosno iz središnje kontrolne točke prema podskupu RPL čvorova. Nadalje, RPL pruža samo osnovnu podršku usmjeravanju od točke do točke tj. između dva RPL čvora.

RPL protokol usmjeravanja usmjerivače organizira prema odredišno usmjerenom acikličkom grafu (engl. DODAG), koji je zadužen za minimiziranje podataka o stanju mreže, a svaki navedeni DODAG nalazi se u različitim odredištima koji se temelje na stablastoj topologiji mreže. Svaki RPL čvor tj. uređaj koji koristi RPL protokol može biti dio najviše jednog DODAG -a, a pomoću navedenog DODAG-i se neće preklapati. Kako bi se uspješno izvršavali različiti zahtjevi usmjeravanja unutar iste komunikacijske mreže, uvodi se RPL

instanca. U osnovi, svaki DODAG unutar iste RPL instance dijeli isti način usmjeravanja, a više instanci RPL-a mogu se izvoditi neovisno o svakoj ostaloj unutar jedne topologije mreže. Slika 28 prikazuje primjer kako RPL čvorovi formiraju DODAG pomoću odgovarajućih čvorova i kako više DODAG-a tvori jednu RPL instancu. Glavna značajka RPL protokola koja ga razlikuje od ostalih definiranih protokola usmjeravanja, način je na koji konstruira rute usmjeravanja. Točnije, rute usmjeravanja konstruira s obzirom na različite QoS zahtjeve korisničkih aplikacija. RPL također ograničava mogućnost čvora da mijenja svoju već definiranu pripadajuću skupinu u DODAG -u te se na taj način uspješno ograničava nestabilnost usmjeravanja [41].



Slika 28. Primjer RPL istance s dva DODAG-a
Izvor: [41]

6.7. Komparativna analiza protokola usmjeravanja u IoT mrežama

U ovom poglavlju prikazana je komparativna analiza protokola usmjeravanja primjenjivih za IoT mreže. U tablici 5 su uspoređeni protokoli usmjeravanja na temelju različitih parametara kao što su npr. klasifikacija protokola, utjecaj protokola na životni vijek mreže, podržavanje agregacije podataka, prilagodljivost na skalabilnost mreže i sl.

Tablica 5. Komparativna analiza IoT protokola

Protokol	*Klasifikacija*	*Životni vijek mreže*	*Agregacija podataka*	*Mobilnost*	*Skalabilnost*	*Upravljanje resursima*
LEACH	Hijerarhijski/proaktivni	Vrlo dobar	Ne	Fiksna bazna stanica	Ograničena	Da
PEGASIS	Hijerarhijski/reaktivni	Vrlo dobar	Da	Fiksna bazna stanica	Dobra	Da
DD	Istorazinski/proaktivni	Dobar	Da	Ograničena	Ograničena	Da
RR	Istorazinski/hibridni	Vrlo dobar	Da	Vrlo ograničena	Dobra	Da
TEEN	Hijerarhijski/reaktivni	Vrlo dobar	Da	Fiksna bazna stanica	Dobra	Da
APTEEN	Hijerarhijski/hibridni	Vrlo dobar	Da	Fiksna bazna stanica	Dobra	Da
GEAR	Lokacijski/proaktivni	Dobar	Ne	Ograničena	Ograničena	Da
GAF	Lokacijski/hibridni	Dobar	Ne	Ograničena	Dobra	Da
ZRP	Hibridni	Vrlo dobar	Da	Ograničena	Dobra	Da
RPL	Temeljen na QoS-u	Vrlo dobar	Da	Vrlo ograničena	Ograničena	Da

Izvor: [29]

LEACH, TEEN, APTEEN i PEGASIS imaju slične značajke i njihove su arhitekture u određenoj mjeri slične, odnosno imaju fiksnu infrastrukturu. LEACH, TEEN, APTEEN su protokoli usmjeravanja temeljeni na klasterima, dok je PEGASIS protokol temeljen na lancu strukture. Performanse APTEEN-a nalaze se između TEEN-a i LEACH-a s obzirom na potrošnju energije i dugovječnost mreže. TEEN prenosi samo kritične podatke, dok APTEEN obavlja periodične prijenose podataka. U tom smislu APTEEN je također bolji od LEACH-a jer APTEEN prenosi podatke na temelju granične vrijednosti dok LEACH prenosi podatke kontinuirano. PEGASIS stvara prekomjerno kašnjenje za udaljene čvorove na lancu. PEGASIS dvostruko povećava životni vijek mreže u usporedbi s LEACH protokolom [29].

DD i RR protokoli koriste metapodatke, dok ih drugi protokoli ne koriste. Budući da su protokoli istorazinskog usmjeravanja, rute se formiraju u regijama koje imaju podatke za prijenos, ostali protokoli koji uglavnom koriste hijerarhijski način usmjeravanja, tvore klastere

po cijeloj mreži. U prethodnom paragrafu protokoli agregaciju podataka vrše unutar glave klastera, dok se prilikom korištenja svih ostalih protokola navedenih u tablici 5 čvorovi na putu višestrukog skoka agregiraju dolazne podatke od susjednog čvora.

Protokoli usmjeravanja DD, RR, GEAR, GAF i RPL ograničeni su u vidu mobilnosti čvorova, no usprkos tome svojim načinom rada imaju za cilj produžiti vijek trajanja mreže. GEAR i GAF za razliku od ostalih protokola mrežu dijele na regije i rešetke kako bi smanjili broj prijenosa podataka i na taj način usavršili usmjeravanje općenito. GEAR ograničava broj interesnih poruka u direktnoj difuziji razmatrajući samo određenu regiju, a ne slanjem interesne poruke cijeloj mreži. GEAR na taj način nadopunjuje DD protokol te štedi više energije [29].

ZRP protokol, kako mu sam naziv govori, temelji se na konceptu zona, što ga u potpunosti razlikuje od svih navedenih protokola u tablici 5. Zona usmjeravanja definirana je za svaki čvor zasebno, dok se zone susjednih čvorova preklapaju.

Glavna značajka RPL protokola koja ga razlikuje od ostalih definiranih protokola usmjeravanja, način je na koji konstruira rute usmjeravanja. Točnije, rute usmjeravanja konstruira s obzirom na različite QoS zahtjeve korisničkih aplikacija [41].

Svrha svih definiranih protokola svakako je produljenje vijeka trajanja mreže i odabir optimalne rute usmjeravanja od izvora do odredišta. S obzirom na dinamičnost i izazove IoT mreža protokoli se dizajniraju u svrhu smanjenja tih izazova, shodno tome u svakom slučaju protokol mora odgovarati području primjene te biti „snalažljiv“ u smislu energetske potrošnje.

7. Zaključak

Neprestani razvoj tehnologija, ujedno poboljšava i sam razvoj IoT koncepta što omogućuje njegovu široku primjenu u različitim sektorima poput zdravstva, prometa, energetike, poljoprivrede, logistike i brojnih drugih u svrhu poboljšanja razine kvalitete života i gospodarskog aspekta. IoT koncept definiran je kao mreža koja može prikupljati i kontrolirati informacije i objekte iz fizičkog svijeta putem različitih uređaja sa sposobnošću opažanja, računanja, izvršavanja radnji i komunikacije. Također se smatra mrežom koja podržava komunikacije između uređaja i čovjeka te između uređaja i uređaja, prijenosom, klasifikacijom i obradom informacija.

IoT koncept primjenjiv je za različita okruženja pomoću niza aplikacija koje proizvode velike količine podataka koje je potrebno prenositi, obrađivati i pohraniti na željeno odredište, a iz tih prikupljenih podataka generirat će se zahtijevane inteligencije koje mogu biti od koristi za izgradnju pametnog okruženja.

U IoT mrežama, sigurno usmjeravanje igra bitnu ulogu u uspješnom i sigurnom funkcioniranju cijele mreže. Različitim kategorizacijama protokola koji se trenutno koriste za usmjeravanje u IoT mrežama nedostaju odgovarajuće sigurnosne implementacije i komponente. Pomoću protokola usmjeravanja potrebno je postići energetski učinkovit sustav za IoT aplikacije gdje bi čvorovi trošili manje snage koja osigurava dugovječnost mreže, sukladno tome potrebno je povećati i propusnost mreže s obzirom na sve veće količine podataka koje se prenose. S obzirom na različite načine usmjeravanja koji su primjenjivi za IoT mreže, protokoli koji su dizajnirani u svrhu usmjeravanja mogu se kategorizirati s obzirom na te načine usmjeravanja. Visoko primjenjivi protokoli su uglavnom oni koji se temelje na mrežnoj strukturi, razlog tome je dinamičnost IoT mreže.

Uz navedenu dinamičnost mreže koja je prikazana kao izazov usmjeravanja, postoji još niz izazova usmjeravanja u IoT mrežama koji su opisani u radu, a uključuju sigurnost, ograničene resurse, ograničenja memorijskih kapaciteta, korištenje niza različitih tehnologija, pohranu i upravljanje velikom količinom podataka te obrada tih podataka kako bi se osigurale korisničke informacija, a samim time i tražena usluga. Pošto se tek očekuje vrhunac razvoja IoT platforme u budućnosti je potrebno uspostaviti snažne baze podataka koje će podnositi i omogućiti pohranu velikih količina korisničkih podataka, također je potrebno poboljšati metode umrežavanja te nadograditi primjenjive komunikacijske tehnologije.

IoT zahtijeva interoperabilnost između korištenih tehnologija, stoga je potrebno smanjiti potrošnju energetskih resursa koje te tehnologije zahtijevaju. Sve tehnologije i protokoli koji su predstavljeni u ovom radu odgovaraju nekim od osnovnih zahtjeva primjene IoT-a, no njihove se karakteristike razlikuju jer je svaka namijenjena za posebne vrste aplikacija i mrežnih topologija. Ipak, neki od predloženih protokola usmjeravanja pomažu u popunjavanju praznina performansi u nekim slučajevima usmjeravanja u IoT mrežama.

IoT je budućnost i potrebno je postaviti snažne baze umrežavanja, poboljšanjem i nadogradnjom odgovarajućih primijenjenih tehnologija. S obzirom da je IoT koncept paradigma koja se i dalje razvija, potrebno je također smanjiti i minimizirati broj izazova koji su prisutni prilikom usmjeravanja.

Literatura

[1] Chen S, Xu H, Liu D, Hu B, Wang H. *A vision of IoT: Applications, challenges, and opportunities with china perspective*. IEEE Internet of Things journal. 2014. Dostupno na: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6851114 [Pristupljeno: srpanj 2021.].

[2] Evans D. *The Internet of Things, How the Next Evolution of the Internet Is Changing Everything*. CISCO; 2011. Dostupno na: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Pristupljeno: srpanj 2021.].

[3] Learn Hub. *5 Essential Components of an IoT Ecosystem*. Dostupno na: https://learn.g2.com/iot-ecosystem [Pristupljeno: srpanj 2021.].

[4] Sureshkumar P.H, Dr. R. Rajesh. *The Analysis of Different Types of IoT Sensors and security trend as Quantum chip for Smart City Management*. IOSR Journal of Business and Management. 2018. Dostupno na: https://www.researchgate.net/publication/322593545_The_Analysis_of_Different_Types_of_IoT_Sensors_and_security_trend_as_Quantum_chip_for_Smart_City_Management [Pristupljeno: kolovoz 2021.].

[5] Enterprise IoT Insights. *What's the difference between an IoT sensor and an IoT actuator?* Dostupno na: https://enterpriseiotinsights.com/20191107/channels/fundamentals/the-difference-between-an-iot-sensor-and-an-iot-actuator [Pristupljeno: kolovoz 2021.].

[6] Dostupno na: https://www.lanner-america.com/blog/what-is-an-iot-gateway/ [Pristupljeno: kolovoz 2021.].

[7] RF Page. *What are the major components of Internet of Things.* Dostupno na: https://www.rfpage.com/what-are-the-major-components-of-internet-of-things/ [Pristupljeno: kolovoz 2021.].

[8] Aman AH, Yadegaridehkordi E, Attarbashi ZS, Hassan R, Park YJ. *A survey on trend and classification of internet of things reviews.* Ieee Access. 2020.

[9] Patel KK, Patel SM. *Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges.* International journal of engineering science and computing. 2016.

[10] Sethi P, Sarangi SR. *Internet of things: architectures, protocols, and applications.* Journal of Electrical and Computer Engineering. 2017. Dostupno na: https://www.hindawi.com/journals/jece/2017/9324035/#B42 [Pristupljeno: kolovoz 2021.].

[11] Triantafyllou A, Sarigiannidis P, Lagkas TD. *Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends*. Wireless

communications and mobile computing. 2018. Dostupno na: https://www.hindawi.com/journals/wcmc/2018/5349894/ [Pristupljeno: kolovoz 2021.].

[12] BEHRTECH. *6 leading types of iot wireless tech and their best use cases.* Dostupno na: https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/ [Pristupljeno: kolovoz 2021.].

[13] ORBCOMM. Dostupno na: https://blog.orbcomm.com/what-the-next-stage-of-the-iot-means-for-supply-chain-management/ [Pristupljeno: kolovoz 2021.].

[14] Perwej Y, Haq K, Parwej F, Mumdouh M, Hassan M. *The internet of things (IoT) and its application domains.* International Journal of Computer Applications. 2019.

[15] Singh PP, Khosla PK, Mittal M. *Energy conservation in IoT-based smart home and its automation*. Energy conservation for IoT devices. 2019. Dostupno na: https://www.researchgate.net/publication/333272298_Energy_Conservation_in_IoT-Based_Smart_Home_and_Its_Automation [Pristupljeno: kolovoz 2021.].

[16] Singh A. *Applications of IoT in Agricultural System*. International Journal of Agricurtural Science and Food Technology. 2019. Dostupno na: https://www.peertechzpublications.com/articles/IJASFT-6-153.pdf [Pristupljeno: kolovoz 2021.].

[17] Mahbub M. *A smart farming concept based on smart embedded electronics, internet of things and wireless sensor network*. Internet of Things. 2020. Dostupno na: https://www.sciencedirect.com/science/article/abs/pii/S2542660520300044 [Pristupljeno: kolovoz 2021.].

[18] Poluru RK, Naseera S. *A Literature Review on Routing Strategy in the Internet of Things.* Journal of Engineering Science & Technology Review. 2017. Dostupno na: http://www.jestr.org/downloads/Volume10Issue5/fulltext61052017.pdf [Pristupljeno: kolovoz 2021.].

[19] Truong CD. *Routing and Sensor Searach in the Internet of Things* (Doctoral dissertation, University of Lübeck). 2014. Dostupno na: https://d-nb.info/1050911814/34 [Pristupljeno: kolovoz 2021.].

[20] Dhumane A, Prasad R. *Routing challenges in internet of things*. CSI Communications. 2015. Dostupno na: https://www.researchgate.net/publication/291074948_Routing_Challenges_in_Internet_of_Things [Pristupljeno: kolovoz 2021.].

[21] Saleem TJ. *A Detailed Study of Routing in Internet of Things*. International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 5. 2016.

[22] Tawalbeh LA, Muheidat F, Tawalbeh M, Quwaider M. *IoT Privacy and security: Challenges and solutions.* Applied Sciences. 2020. Dostupno na: https://www.mdpi.com/2076-3417/10/12/4102 [Pristupljeno: kolovoz 2021.].

[23] Durairaj M, Asha HM. *The Internet of Things (IoT) Routing Security—A Study*. Research Gate. Dostupno na: https://www.researchgate.net/publication/339703110_The_Internet_of_Things_IoT_Routing_Security-A_Study [Pristupljeno: kolovoz 2021.].

[24] Farooq MU, Waseem M, Mazhar S, Khairi A, Kamal T. *A review on internet of things (IoT).* International journal of computer applications. 2015.

[25] Porkodi R, Bhuvaneswari V. *The internet of things (IOT) applications and communication enabling technology standards: An overview.* International conference on intelligent computing applications. 2014. IEEE.

[26] Aldowah H, Rehman SU, Umar I. *Security in internet of things: issues, challenges and solutions.* InInternational Conference of Reliable Information and Communication Technology. 2018. Dostupno na: https://www.researchgate.net/profile/Hanan-Aldowah/publication/326579980_Security_in_Internet_of_Things_Issues_Challenges_and_Solutions/links/5bf7ba1592851ced67d15f31/Security-in-Internet-of-Things-Issues-Challenges-and-Solutions.pdf
[Pristupljeno: kolovoz 2021.].

[27] Poluru RK, Naseera S. *A Literature Review on Routing Strategy in the Internet of Things*. Journal of Engineering Science & Technology Review. 2017. Dostupno na: http://www.jestr.org/downloads/Volume10Issue5/fulltext61052017.pdf [Pristupljeno: kolovoz 2021.].

[28] Ques10. Dostupno na: https://www.ques10.com/p/50443/flat-versus-hierarchical-routing-protocols/? [Pristupljeno: rujan 2021.].

[29] Bhattacharyya D, Kim TH, Pal S. *A comparative study of wireless sensor networks and their routing protocols.* Sensors. 2010. Dostupno na: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3231091/ [Pristupljeno: rujan 2021.].

[30] Braginsky D, Estrin D. *Rumor routing algorthim for sensor networks*. International workshop on Wireless sensor networks and applicationsy. 2002 Dostupno na: https://www.researchgate.net/publication/220926359_Rumor_Routing_Algorithm_for_Sensor_Netowrks [Pristupljeno: rujan 2021.].

[31] Pathak S, Sharma B. *A Comparative Analysis of Routing Protocols in IoT*. International Conference on Computing for Sustainable Global Development (INDIACom). 2019.

[32] Researchgate. Dostupno na: https://www.researchgate.net/figure/LEACH-protocol-phases_fig2_327289160 [Pristupljeno: rujan 2021.].

[33] Haseeb K, Islam N, Almogren A, Din IU, Almajed HN, Guizani N. *Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs*. IEEE Access. Dostupno na: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8736739 [Pristupljeno: rujan 2021.].

[34] Researchgate. Dostupno na: https://www.researchgate.net/figure/Data-gathering-at-head-node-in-PEGASIS-protocol_fig2_221193273 [Pristupljeno: rujan 2021.].

[35] Khedr AM, Aziz A, Osamy W. *Successors of PEGASIS protocol: A comprehensive survey*. Computer Science Review. 2021. Dostupno na: https://www.sciencedirect.com/science/article/pii/S1574013721000083?dgcid=rss_sd_all [Pristupljeno: rujan 2021.].

[36] Manjeshwar A, Agrawal DP. *TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks*. Inipdps. 2001. Dostupno na: http://www.njavaid.com/TEEN.pdf [Pristupljeno: rujan 2021.].

[37] Researchgate. Dostupno na: https://www.researchgate.net/figure/GEAR-B-Classification-based-on-Protocol-Operation-Depending-on-the-protocol-operation_fig4_295595436 [Pristupljeno: rujan 2021.].

[38] Ai ZY, Zhou YT, Song F. A smart collaborative routing protocol for reliable data diffusion in IoT scenarios. Sensors. 2018.

[39] Aznaoui H, Raghay S, Aziz L. *Location-based routing protocols gaf and its enhanced versions in wireless sensor network a survey*. International Journal of Computer Science and Information Security. 2016. Dostupno na: https://www.semanticscholar.org/paper/Location-Based-Routing-Protocols-GAF-and-its-in-a-Aznaoui-Raghay/c8adbe4a0de56c1f57b5a1ff652c022f41de0f41/figure/1 [Pristupljeno: rujan 2021.].

[40] Beijar N. *Zone routing protocol (ZRP)*. Networking Laboratory, Helsinki University of Technology, Finland. 2002. Dostupno na: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.19.5568&rep=rep1&type=pdf [Pristupljeno: rujan 2021.].

[41] Ancillotti E, Bruno R, Conti M. *The role of the RPL routing protocol for smart grid communications*. IEEE Communications Magazine. 2013. Dostupno na: https://core.ac.uk/download/pdf/37831692.pdf [Pristupljeno: rujan 2021.].

Popis kratica

IoT	Internet of Things
RFID	Radio-frequency identification
NFC	Near-field communication
Wifi	Wireless Fidelity
GPS	Global Positioning System
OSI model	Open System Interconnection – Reference Model
TCP/IP	Transmission Control Protocol/ Internet Protocol
UMTS	Universal Mobile Telecommunications System
WSN	Wireless Sensor Network
QR	Quick Response code
MEMS	Micro-Electro-Mechanical Systems
SPIN	Sensor Protocol for Information via Negotiation
DD	Directed Diffusion
RR	Rumor Routing
MCFA	Minimum Cost Forwarding Algorithm
LEACH	Low Energy Adaptive Clustering Hierarchy
PEGASIS	The power-efficient gathering in sensor information systems
RPL	Routing Protocol for Low-Power and Lossy Networks
SOP	Self Organizing Protocol
TEEN	Threshold sensitive Energy Efficient sensor Network protocol
APTEEN	Adaptive Threshold-sensitive Energy Efficient Network
VGA	Virtual Grid Architecture
GAF	Geographic Adaptive Fidelity
LPBR	Location Prediction Based Routing Protocol
SPAN	Switch Port Analyzer
GOAFR	Greedy Other Adoptive Face Routing
AODV	Ad-hoc on-demand distance vector routing system
DSR	Dynamic source routing
TORA	Temporarily ordered routing algorithm
SEER	Spectrum and Energy Efficient routing protocol
OLSR	Optimized linked state routing
DSDV	Destination sequenced distance vector

TBRPF	Topology dissemination based on reverse path forwarding
GPSR	Greedy Perimeter Stateless Routing
ZRP	Zone based routing protocol
SOC-M2M	Self-Organized Clustering Machine-to-Machine
AOMDV	Ad-hoc on demand Multipath Distance Vector
DSDV	Destination Sequence Distance Vector
HEED	Hybrid Energy Efficient Distributed Clustering
GEAR	Geographic and Energy Aware Routing
RPL	Routing Protocol for Low-Power and Lossy Networks
SAR	Sequential assignment routing
TDMA	Time-division multiple access
CDMA	Code-division multiple access
IETF	The Internet Engineering
DODAG	Destination Oriented Directed Acyclic Graph

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski 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 diplomskog rada pod naslovom

Analiza izazova i pristupa kod usmjeravanja u mrežama *Internet of Things*

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 9.9.2021

Jelena Perić

(potpis)