Sustavi za umrežavanje uređaja u pametnom domu

Kukec, Matija

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU

STRUČNI STUDIJ RAČUNARSTVO

MATIJA KUKEC

SUSTAVI ZA UMREŽAVANJE UREĐAJA U PAMETNOM DOMU

ZAVRŠNI RAD

ČAKOVEC, 2021.

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU

STRUČNI STUDIJ RAČUNARSTVO

MATIJA KUKEC

SUSTAVI ZA UMREŽAVANJE UREĐAJA U PAMETNOM DOMU

SYSTEMS FOR DEVICE NETWORKING IN A SMART HOME

ZAVRŠNI RAD

Mentor:

struč. spec. ing. techn. inf. Robert Poljak, pred.

ČAKOVEC, 2021.

Zahvala

Želio bih zahvaliti svim profesorima Međimurskog veleučilišta u Čakovcu koji su mi pomogli u stjecanju znanja, a posebice svojem mentoru na pomoći i razumijevanju tijekom izrade završnog rada. Veoma sam zahvalan svojim kolegama uz koje sam studirao, a osobito djevojci i obitelji koji su također bili velika podrška.

SAŽETAK

Pametna kuća ili pametni dom je sustav koji nadgleda, odnosno „osluškuje“ svojim osjetilima, tj. senzorima, a zatim prema postavkama korisnika i/ili statistikom prikupljenih podataka i algoritmima kontrolira funkcije, odnosno atribute u kućanstvu poput klime, rasvjete, medijskih uređaja i slično. Motivacije za kreiranje i korištenje pametnog doma polaze prvobitno od napretka tehnologije općenito i nekih društvenih promjena i trendova koji se događaju pri čemu se pojavljuje sve više pametnih uređaja te raznoraznih jeftinijih senzora i modula. Štoviše, koncept pametne kuće pojavio se još 1900-ih godina uvođenjem kućanskih aparata za olakšavanje života i pojave struje. Većina vrijednosti pametnog doma proizlazi iz samog okruženja, a ne od vrste tehnologije koja se koristi, načina na koji su uređaji postavljeni u pametnom domu i načina na koji oni zajedno funkcioniraju. Kako tehnologija raste, sve je više uređaja koji pronalaze mjesto u našim domovima, no korisnici pametnih domova ne žele poseban daljinski upravljač za svaki od tih uređaja, već žele da oni imaju zajedničko sučelje gdje su integrirani i funkcioniraju besprijekorno.

Kreiranje pametnog doma, osim pružanja udobnosti i olakšavanja svakodnevnih zadataka, može pomoći, odnosno pružati potporu ljudima s invaliditetom te starijim i nemoćnim osobama. Algoritmima za promicanje štednje energije u pametnom domu također utječemo i na okoliš. Npr. upravljanjem uređajima za grijanje vode, rashlađivanje prostora ili gašenje svjetala kad određeno vrijeme nitko nije u kući i slično. Očito je da pridonosi smanjenju troškova za život korisnika te istovremeno nudi udobnost u pametnom domu. U svakom slučaju naglasak je na poboljšanju kvalitete života. Uspoređivat će se umrežavanje uređaja metodom otvorenog koda i komercijalnom metodom sustava umrežavanja u pametnom domu. Odnosno, propitat će se u kojim slučajevima Raspberry Pi kao mrežni usmjerivač ili općenito projekti otvorenog koda za ZigBee protokol pobjeđuju. Dakle, usporedit će se pristupačnost takvih metoda i sustava na tržištu, težina osnovne konfiguracije i ono najbitnije, pouzdanost.

Ciljana ideja bila bi iskoristiti ZigBee u praksi kao jednog od navedenih protokola za komunikaciju unutar kućne instalacije raznih uređaja te pritom

istražiti i opisati način na koji komuniciraju, počevši od fizičkog sloja, pa sve do same strukture paketa koji se šalju, kao i ostvarivanja početne konfiguracije, adresiranja i upravljanja tim sustavom, a na kraju i aplikacijski sloj i sučelje za interakciju s uređajima.

Ključne riječi: *ZigBee, internet stvari, lokalna mreža, računala, pametni dom*

SADRŽAJ

1. UVOD

Termin pametni dom poznat je i pod nazivom domotika (engl. *Domotica*) što doslovno znači kućna robotika; derivacija od latinske riječi za dom (lat. *domus*) i engleske riječi za robotiku (engl. *robotica*), a opis je sustava nekog prebivališta koji zna stanja svojih uređaja umreženih u centar/upravljač pametnog doma koji spaja sve pametne uređaje u mrežu [1]. Većina velikih proizvođača opreme za pametni dom pruža kupcima neki univerzalni koncentrator koji služi kao čvorište ostalim uređajima.

U računarstvu i računalnim znanostima postoji koncept sveprisutnog računarstva koji podrazumijeva da se računarstvo pojavljuje bilo kad i bilo gdje, a blisko je povezan s pojmom internet stvari (engl. *Internet of Things*), odnosno IoT-om koji po definiciji predstavlja mrežnu infrastrukturu u kojoj fizičke i virtualne „stvari“ svih vrsta komuniciraju i nevidljivo su integrirane. Zahvaljujući rapidnom napretku tehnologije, IoT je moguće integrirati u sve više uređaja.

U današnjim sustavima koncentrator se spaja u kućni usmjernik i time se povezuje konvencionalnim TCP/IP protokolom. Također, postoje rješenja s kupljenim modulom koji se onda spaja na određeno računalo gdje sustav vrti okruženje u VM-u ili nekoj aplikaciji, web serveru i na taj način pruža usluge upravljanja uređajima i postavljanja automatizacije.

Kada govorimo o sustavima za umrežavanje uređaja u pametnom domu, postoje mnoge opcije koje možemo iskoristiti za spajanje pametnih uređaja od kojih su neke nekonvencionalne i zastarjele metode poput korištenja električnih instalacija ili biranja radiovalova kao komunikacije u određenim radijskim frekvencijama i pojasevima. No, što se tiče bežičnog umrežavanja, većinom govorimo o izboru između nekoliko najčešće korištenih protokola, a to su WiFi, Z-Wave i onaj kojeg ćemo se pobliže dotaknuti u ovom radu: ZigBee. U radu će biti pokrivene različite teme kao što su: usporedba karakteristika različitih protokola (poput frekvencijskih spektara), testiranje propusnosti, vremenskih odaziva paketa, potrošnje energije te sama građa paketa i njihovih korisničkih podataka korisne nosivost (engl. *payload*).

2. PODRUČJA PRIMJENE

Gotova rješenja za pametnu kuću postoje i mogu se kupiti u trgovini i često dolaze s nekim od uređaja kao što su senzori pokreta, kamere za videonadzor, pametne žarulje, termostati, pametne utičnice i slično. Oni omogućavaju samostalnu instalaciju uređaja, upravljanje temperaturom i svjetlom u domu kao i praćenje događanja tijekom odsustva vlasnika.

Područja primjene ZigBee tehnologije su mnoge, a ovo su neka od njih [2]:

- Grijanje, ventilacija i klimatizacija (engl. HVAC): moguće je daljinsko upravljanje mikroklimom.
- Sustav kontrole rasvjete: pametna mreža koja uključuje komunikaciju između različitih ulaznih i izlaznih parametara rasvjetnih sustava.
- Zdravstveni sustavi: kontrola tlaka, mjerenje koncentracije glukoze u krvi, pulsa, tjelesne temperature.
- Kontrolni sustav koji je svjestan zauzetosti prostora (engl. *Occupancy-aware control system*) i koji pomoću pametnih senzora prati kvalitetu zraka, poput CO_2 senzora, mikroklime i sl. te prema tome podešava parametre mikroklime u prostoriji u kojoj se nalaze osobe čime čini pametni dom energetski učinkovitim.
- Primjena kontrole u integraciji solarnih panela i pametnih vodova. Primjerice, mjerenjem izlazne energije pametni sustav može odrediti u koje je doba dana najučinkovitije uključiti određeni kućanski aparat kako bi se potrošio višak proizvedene energije.
- Pametni kućni roboti i sigurnosni sustavi.
- Unutarnji sustav pozicioniranja (engl. IPS – *Indoor positioning system*).
- Automatizacija doma za starije i nemoćne.
- Senzori potresa.
- Sustavi nadgledanja djece i kućnih ljubimaca.
- Pametna kuhinja: pametni štednjaci, frižideri, nape…

3. KORISNIČKA SUČELJA

Uređaje u pametnoj kući pokreću, nadziru i kontroliraju određeni procesi kuće na temelju programiranja, a ovisno o scenariju. Iza tih radnji mora stajati određena tehnologija, a kako bismo počeli umrežavati svoje uređaje u pametnom domu, potrebno je glavno čvorište. Koncentrator služi kao čvorište, a radi na jednoj od odabranih tehnologija i ima određenu programsku podršku koja se izvodi kako bi korisnik komunicirao i upravljao automatizacijom uređaja.

Programska potpora koja se izvodi na računalu jedna je od bitnijih komponenti u sustavu jer daje mnogo opcija korisniku. Postoji mnogo projekata otvorenog koda, a uz to postoje gotovi proizvodi za komercijalnu uporabu. Kod proizvoda komercijalne uporabe treba napomenuti da se pojavljuje problem kompatibilnosti između jednog i drugog proizvođača jer u svakoj kući postoje prekidači za svjetla, prekidači za garažna vrata, prekidači za električnu ogradu, raznorazni daljinski upravljači itd. Tako postoje i sučelja za upravljanje pametnim domom.

X10 protokol koji je industrijski standard, odnosno komunikacijski protokol za kućnu automatizaciju električnih uređaja koji koriste primarno električne kućne instalacije koje su se ujedno koristile za signaliziranje i kontrolu pomoću kratkih radiosignala u izmjeničnoj struji i time su predstavljale prijenos informacije. X10 je razvijen 1975., a na slici 1. predstavljeni su X10 upravljači.

Slika 1. X10 upravljači: jednostavan upravljač, radioupravljač i originalna konzola za naredbe koja se može koristiti s ultrazvučnim daljinskim upravljačem [3]

Nekad su to bile glomazne kontrolne ploče, no danas se uglavnom koriste zasloni na dodir kao sučelja za pametni dom, poput tableta koji služi kao kontrolna ploča ili pametnog telefona. Korisnici danas imaju razne opcije kako koristiti sučelje za upravljanje.

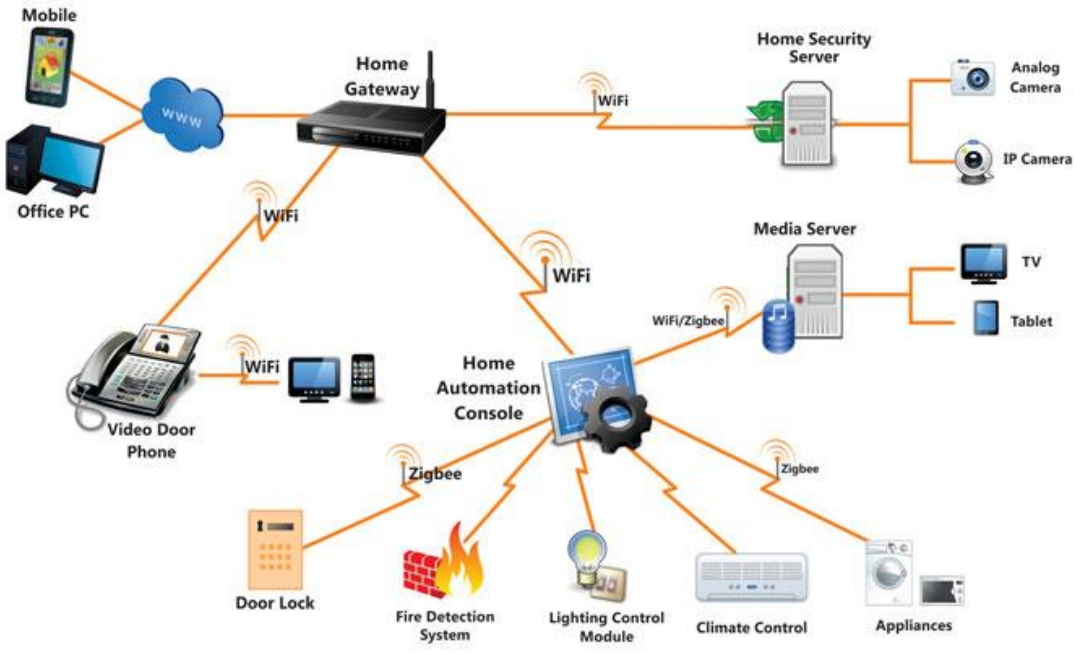
4. TOPOLOGIJA MREŽE PAMETNOG DOMA

Važno je i o kakvoj je topologiji mrežnog sustava riječ te jesu li uređaji dostupni putem daljinske usluge izvan mreže doma. Mreža kuće može biti izvedena poput VLAN-a na način da se podijeli na više virtualnih privatnih mreža, u drugačijoj podmreži (engl. *subnet*), te na taj način osigurava susjedne VLAN mreže ako dođe do proboja na jednoj od slabih točaka/uređaja u pametnom domu. Konfiguracijom na vatrozidu (engl. *firewall*) usmjerivača možemo poboljšati sigurnost na način da propušta samo određeni promet.

Topologija mreže pametnog doma mora biti postavljena sukladno sigurnosnim standardima kako ne bi došlo do neželjenih posljedica poput malicioznih napada s opasnog interneta. Svaki korisnik isto tako želi i očekuje udobnost u svome domu. No ovdje dolazi do suprotnosti jer slobodni, nesmetani rad i puna iskorištenost svih značajki koje umreženi uređaji u pametnom domu iziskuju, često nisu u skladu sa sigurnosnim mjerama. Stoga možemo slobodno reći da su pojmovi sigurnost i komfor u suprotnosti, kao i inače u životu. Način na koji radimo sklad između sigurnosti i udobnosti je smještanje uređaja na pravo mjesto, tj. VLAN i postavljanje pravila u mreži, tj. kontrola prometa.

IoT uređaji mogu se podijeliti u četiri glavne kategorije:

- uređaji koji trebaju komunicirati s uslugom u oblaku izvan lokalne mreže
- uređaji koji komuniciraju samo unutar lokalne mreže
- uređaji koji trebaju razgovarati s uslugom u oblaku i uređajima na lokalnoj mreži
- nepouzdani uređaji, tj. uređaji koji uopće ne trebaju izlaznu komunikaciju, a trebali bi govoriti samo kada im se pošalje zahtjev.



Slika 2. Topologija kućne mreže uključujući ZigBee automatizaciju [10]

Daljinski pristup omogućuje nam pristupanje sučelju pametnog doma gdje geografska lokacija ne predstavlja problem ako postoji pristup mreži svih mreža. Samo u ovom slučaju gdje Raspberry Pi služi kao glavni poslužitelj za sve umrežavanje uređaja putem Homeassistant sučelja, već postoje mnogobrojne opcije za pristup putem web preglednika iz mreže svih mreža. Postoji dakako više opcija, ali glavni i najjednostavniji načini za omogućavanje daljinskog pristupa su primjerice:

1. Postavljanje obrnutog posredničkog poslužitelja (engl. *proxy server*). Takvo rješenje je primjerice *NabuCasa* koji funkcionira kao obrnuti *proxy*. Jedan je od mnogih komercijalnih rješenja, no jednostavan za korištenje [4].
2. Otvaranje, odnosno otkrivanje obrnute *proxy* opcije prosljeđivanja portova s dodatnim slojem autentifikacije. Ne preporuča se otkrivati svaki servis direktno.
3. Nikada se ne preporuča prosljeđivanje porta 22. na ruteru, već se umjesto toga preporuča otvaranje nasumičnog porta visokog broja.

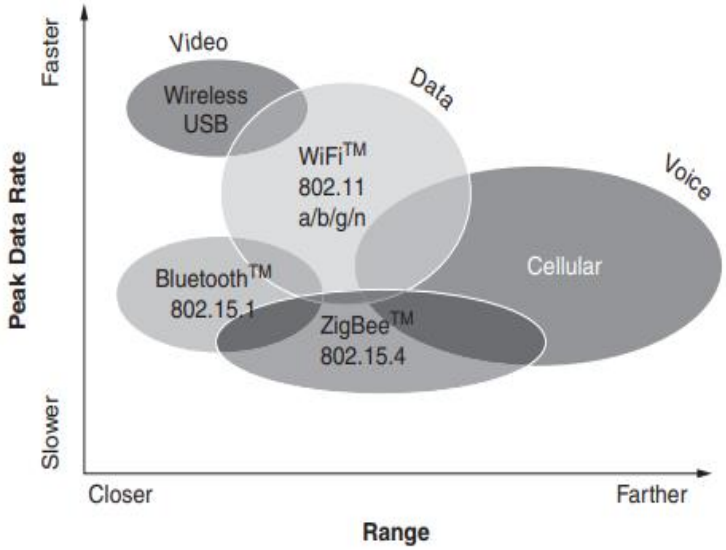
Time se spašava sigurnosno pitanje i bezbrojnih *brute force* pokušaja i obavijesti o tisuću neuspješnih prijava.

4. Može se i direktno pristupati web sučelju Homeassistanta putem SSH-a korištenjem *socks5* tuneliranja.
5. Pristup spajanju na virtualnu privatnu mrežu je najbrži, najsigurniji i najefektivniji način spajanja do Homeassistant poslužitelja (u ovom slučaju Raspberry Pi) koji obitava na lokalnoj mreži pametnog doma.

U svakom se slučaju preporuča korištenje statične IP adrese i DNS servisa kako bi se dobila domena. Na taj način pojednostavljuje se način instalacije i korištenja daljinskog pristupa umreženom sustavu u pametnom domu. Isto tako vrijedi spomenuti da će većina pružatelja usluga pristupa internetu (engl. ISP – *Internet Service Provider*) blokirati portove 80 i 443 za nadolazeći promet koji putuje prema računalu internetskom vezom – uglavnom se može zamoliti pružatelje da maknu to ograničenje, no postoji protokol koji se zove CGNAT (engl. *Carrier Grade NAT*) koji se koristi kako bi svi njihovi umreženi uređaji bili iza većeg usmjerivača kojim kolaju podaci preko internetske veze. Prevođenje mrežnih adresa ili NAT (engl. *Network Address Translation*) omogućuje nam upotrebu iste javne (vanjske) IP adrese za više privatnih (internih) IP adresa istovremeno. Dok će se, zahvaljujući CGNAT-u, tvrtke s više istovremeno povezanih računala moći povezati na internet koristeći vrlo malo IP adresa [5]. Dakle, javna IP adresa koju računalo koristi može biti primjerice 195.82.12.122 na CGNAT-u, ali ustvari sav promet koji izlazi, zapravo izlazi kroz javnu adresu 195.90.10.1. Poanta je da je prosljeđivanje portova na CGNAT-u zahtjevnije zbog toga što promet prolazi kroz najmanje tri usmjerivača zbog čega su pravila filtracije prometa rigoroznija.

5. ZIGBEE

Od bežičnih standarda postoje već WiFi, Bluetooth, mobilne mreže, WiMAX, RFID, Wibree itd. Zašto ZigBee? ZigBee je bežični standard koji spada u područje koje ostale mreže ne pokrivaju u smislu dometa i brzine prijenosa podataka.



Slika 3. Usporedba bežičnih tehnologija prema dometu i propusnosti [6]

Na grafu možemo vidjeti tehnologije uspoređene na temelju dometa i brzine prijenosa podataka gdje su Wireless USB i WiFi za brži prijenos podataka na bližoj udaljenosti, a Bluetooth koji se koristi za *handsfree* uporabu ima nešto sporiji prijenos podataka. S desne strane grafikona vidljiva je sekcija mreže za mobilnu telekomunikaciju koja obuhvaća odličan geografski raspon i u nekom prosjeku srednju brzinu prijenosa podataka, ali je vrijeme odaziva vjerojatno nešto slabije u odnosu na one koji su bliže. ZigBee se smjestio ispod svih područja, ali pokriva bliže i dalje daljine, nešto više od WiFi tehnologije, a manje od mobilne telekomunikacije, no ima vrlo niske brzine prijenosa podataka [5].

Norveška legenda o ZigBeeju:

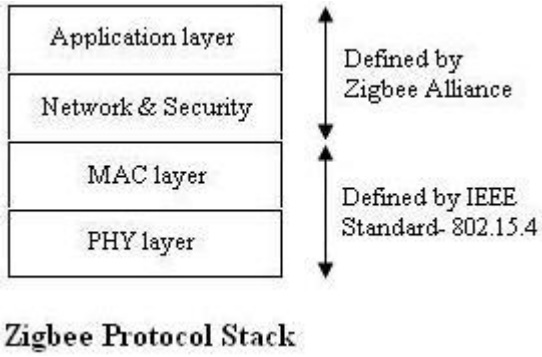
„Norveška legenda govori o malom trolu pod imenom ZigBee koji je živio u selu Vik daleko u unutrašnjosti na fjordu Sogn. Norveški trolovi nisu velika, gadna i smrdljiva, tvrda kao stijena sorta o kojoj se često priča u drugim pričama, barem ne uvijek. ZigBee je bio ljubazan, tihi mali trol koji nije puno govorio, ali kad je govorio, uvijek je bio pouzdan. Osoba je mogla računati na ZigBeeja. Jednom je ZigBee osjetio da je hrpa sijena naslagana na Barnesu postala prevruća i počela je tinjati. ZigBee je začas oglasio alarm u svakoj kući u selu i seljani su mogli ugasiti požar prije nego što je staja bila izgubljena. Neki drugi dan djed je na svom malom ribarskom brodu napustio luku Vik i Sogn kako bi s unukom Britom ulovio lososa. Taj dan, za razliku od ostalih, Brita nije bila oprezna. Bestefar (norveški naziv za djeda) nije primijetio kad je Brita pala preko palube jer je bio zauzet izvlačenjem mreže pune ribe s krme malog čamca. ZigBee, osjetivši da je Brita pala, upozorio je Bestefara i on ju je uspio spasiti od utapanja.

Još je jedmom ZigBee spasio cijelo selo Vik.. Lokalni seljanin zvani Haarold Bluetooth bio je daleko u zasnježenim planinama čuvajući svoje stado ovaca u rano proljeće. Te je godine bilo toplo proljeće, nakon posebno teške zime. Pastir Bluetooth doveo je svoje stado do potoka koji je dobro poznavao, ali ove godine nije mu mogao prići. Potok se od brzo topljenog snijega pretvorio u poplavnu rijeku. Uzrujan, Bluetooth je poželio stanovnike sela upozoriti na poplavu prije nego stigne do sela, ali selo je bilo predaleko da bi ga netko mogao čuti. Bluetooth jednostavno nije imao domet da pomogne selu. ZigBee, osjetivši problem, vidio je poplavu. I ZigBee je, poput Bluetootha, shvatio da je predaleko da bi se mogao čuti i jedan jedini uzvik. Tako je odmah počeo skakati niz planinske izbočine sve dok nije stigao do sela. Automatski je otvorio branu i poplava je prošla bez oštećenja sela.

Vik i Sogn imali su sreće što su imali ZigBeeja i što je ZigBee znao skakati višestruke skokove.“ [6]

Posebna moć ZigBee protokola leži upravo u tome što postoji mogućnost skoka paketa s jednog uređaja na drugi čime se efektivno produljuje mrežni doseg. Do potrebe ZigBee protokola dolazi još 1998. zbog potrebe umrežavanja IoT uređaja s pouzdanošću, potrebe umrežavanja velikog broja uređaja u pametnom domu te zahtjevom za izrazito niskom potrošnjom energije kod komunikacije gdje uređaj može raditi na maloj bateriji napona 3 V, primjerice CR2032 mjesecima. Kao što je već napomenuto, ZigBee ima spor prijenos podataka zbog nepostojeće potrebe za umrežavanje IoT uređaja koji npr. samo kod promjene temperature šalju informaciju o promjeni temperature, potrošnje energije ili slično. Na primjer, nekad korisnik osam puta dnevno pošalje zahtjev da se otvori prekidač za paljenje/gašenje svjetla, a nekada možda ni jednom u danu pa je smisao prepoznati uređaje koji rijetko šalju podatke. ZigBee Alliance stvoren je 2002. godine i 2003. godine postaje standardizirani, globalni i univerzalni protokol za IoT namjene svih spomenutih zahtjeva i time dozvoljava različitim proizvođačima da implementiraju tehnologiju u svoje proizvode.

Iako se ZigBee temelji na IEEE normi 802.15.4, njih ne treba poistovjećivati. Naime, norma 802.15.4 definira specifikacije fizičkog sloja i podsloja za upravljanje vezama MAC (engl. *Medium access control*) za niskopropusne bežične komunikacije fiksnih, prijenosnih i pokretnih uređaja bez i s baterijom koje zahtijevaju nisku potrošnju, LR-WPANs (engl. *Low-rate wireless personal area networks*).



Slika 4. Podjela ZigBee stoga [13]

Dodatno, standard pruža načine rada koji omogućuju precizno određivanje položaja u prostoru [6], pa prema tome ZigBee Alliance i 802.15.4 standard imaju sličan odnos kao i 802.11 standard i WiFi Alliance.

ZigBee Alliance napravio je vrlo jeftin, učinkovit, bežični standard za dvosmjernu komunikaciju. Također, mnoštvo literature pokušava objasniti ZigBee protokol na način da brojne tvrtke koje implementiraju ZigBee standard u svoje proizvode na temelju jedinstvenih pravila protokola proizvedu jeftine, međusobno interoperabilne proizvode koji su vrlo upotrebljivi i zadovoljavaju zahtjeve korisnika na tržištu bežičnih proizvoda koje danas buja [7].

5.1 Podjela ZigBee uređaja po funkcionalnosti

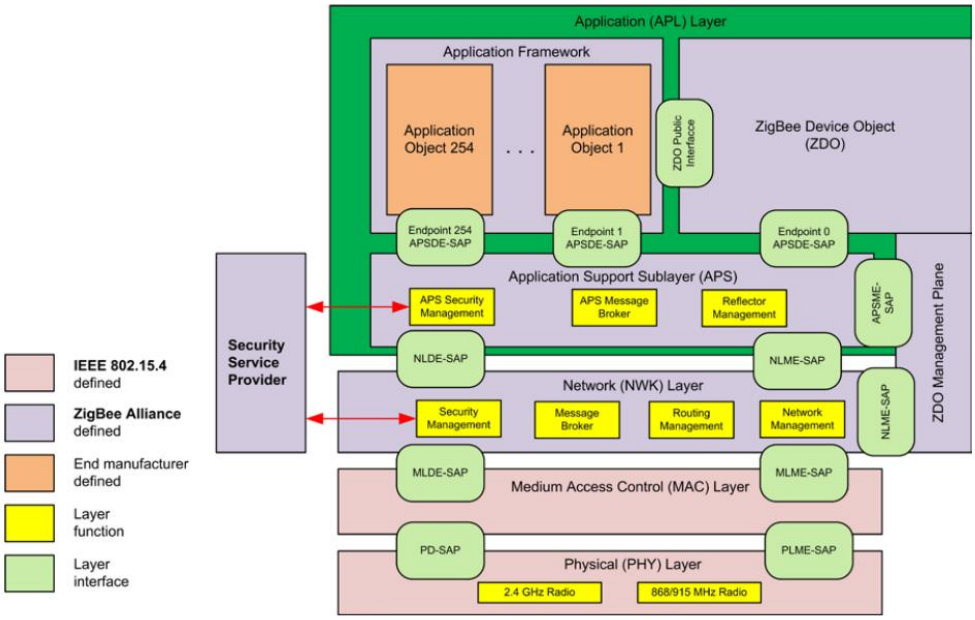
Dvije klase uređaja definirane su po funkcionalnosti: FFD (engl. *Fully Functional Device* – uređaj s potpunom funkcionalnošću) klasa i RFD (engl. *Reduced Functional Device* – uređaj s ograničenom funkcionalnošću) klasa. Klasa FFD uređaja uglavnom je spojena na neki stalni izvor napajanja i usmjeruje pakete, dok su klase RFD uređaja energetski samostalne (tj. imaju neko vlastito autonomno napajanje) te su kao takve ograničene u energetskom smislu i funkcija mreža pa su prema tome krajnji čvorovi koji ne usmjeruju, tj. ne prosljeđuju pakete.

ZigBee uređaji dijele se po funkcijama na:

- Mrežni ZigBee koordinator koji je uvijek FFD. On obavlja inicijalizaciju mreže, dakle uspostavlja vezu između ostalih čvorova i zna gdje se koji nalazi i kako doći do kojeg uređaja. Ostvaruje PAN (engl. *Personal Area Network*) ili, slobodno prevedeno, osobnu računalnu mrežu, stoga on odabire PAN ID i frekvenciju, odnosno kanal mreže. Nema stanja mirovanja i napajanje mu je iz utičnice. Može služiti i kao izlaz prema nekoj drugoj vrsti mreže (LAN, GSM itd.).
- Usmjerivač (engl. *router*) također je uvijek FFD i služi za povećanje dometa mreže. Nema načina štednje energije ili stanje mirovanja i isto mu je napajanje iz utičnice.
- I na kraju, postoji krajnji uređaj ili krajnji čvor koji je uglavnom RFD, a može i ne mora biti FFD. Na njemu su uglavnom smještena osjetila, aktuatori ili neke upravljačke jedinice [7]. Ne mogu dopuštati drugim uređajima da se spoje na PAN niti mogu asistirati usmjerivanju kroz mrežu. Podržava način rada koji štedi energiju, može ići u duboko stanje mirovanja.

6. ZIGBEE OSI MODEL

ZigBee protokolni stog temelji se na OSI modelu, ali ne prati konvencionalni 7-slojni model, već ima samo neke iste elemente i definira samo one slojeve važne za ostvarivanje funkcionalnosti na željenom području, a to su fizički sloj (PHY), sloj za pristup mediju (MAC) i mrežni sloj (NWK). Slojevi od 4 do 7 (transportni, sesijski, prezentacijski i aplikacijski sloj) upakirani su zajedno u aplikacijski sloj (APL) u kojem su naslagani aplikacijski okviri (engl. *Application Framework*), objekt ZigBee uređaja (engl. ZDO – *Zigbee Device Object*) i aplikacijski podsloj za podršku (engl. APS – *Application Support Sublayer*) [8].



Slika 5. Arhitektura OSI modela ZigBee protokola [8]

6.1 Fizički sloj

Uloga fizičkog sloja - PHY (engl. *physical layer*), jest aktivacija ideaktivacija primopredajnika, mjerenje razine energije signala – ED (engl. *Energy Detection*), indikacija kvalitete veze - LQI (engl. *Link Quality Indicator*), provjera i angažiranje kanala koji je slobodan - CCA (engl. *Clear Channel Assesment*), odabir kanala te primanje i slanje podataka putem elektromagnetkih valova. Prema IEEE 802.15.4 fizički sloj djeluje u industrijskom, znanstvenom i medicinskom (ISM) opsegu. Omogućuje prijenos i prijem podataka, modulaciju odlaznih signala i demodulaciju dolaznih signala te upravlja funkcijom primopredajnika (odašiljača i prijamnika). Definira tri pojasa frekvencija: od kojih jedan radi na 868 MHz koji se koristi u Europi, u rasponu od 868 do 868,6 MHz i podržava prijenos podataka od 20 kbps, drugi na 915 MHz s 10 kanala (1 – 10) i brzinom prijenosa od 40 kbps te treći na 2,4 GHz sa 16 kanala (11 – 26) s brzinom prijenosa od 250 kbps i širinom kanala od 5 MHz. Na prva dva pojasa koristi se binarna PSK (engl. *Phase Shift Keying*) modulacija, dok se na trećem pojasu koristi OQPSK (engl. *Offset Quadrature Phase Shift Keying*). U frekvencijskom opsegu na 2,4 GHz deklarirani domet u otvorenom prostoru iznosi do 100 m, dok u zatvorenom iznosi 30 m pri snazi odašiljanja od 1 do 100 mW. Radi poboljšanja odnosa signal/šum te povećanja selektivnosti kanala upotrebljava se tehnika moduliranja raspršenja spektra direktnim postupkom DSSS, skraćenica od engl. *Direct Sequence Spread Spectrum* [9].

6.2 Sloj za pristup mediju

Sloj za pristup mediju MAC (engl. *Medium Access Layer*) zadužen je za pristup i komunikaciju između fizičkog i mrežnog sloja, generiranje i sinkroniziranje komunikacije, pokretanje koordinatora i generiranje PAN ID-a (engl. *Personal Area Network Identinfier*) i izvršavanje GTS-a (engl. *Guaranteed Time Slot*) koji određuje određeni vremenski okvir za komunikaciju između uređaja u mreži. Koristi CSMA-CA mehanizam za pristup kanalu pa je prema tome nepotpuni dupleks ili poludupleks (engl. *half-duplex*), kao i ostale bežične mreže. Svrha MAC sloja je i uspostavljanje veze između MAC entiteta na različitim čvorovima i ostvarivanje pouzdane komunikacije između dvaju susjednih čvorova u mreži. Funkcionalnost uređaja definirana je na ovom sloju. Također, MAC sloj podržava određene sigurnosne mehanizme.

6.3 Mrežni sloj

Briga mrežnog sloja NWK (engl. *network layer*) je pravilna izgradnja mrežne topologije, konfiguracija uređaja, kao i uključivanje i isključivanje novog ili postojećeg čvora s mreže. Dostavlja poruke adresiranom odredištu kojem je poruka namijenjena, otkriva susjede i stvara putove između dva čvora. Zadužen je za primanje i prosljeđivanje podataka između aplikacijskog i MAC sloja, tj. efektivnu obradu podataka između dva sloja. Mrežni sloj podržava usmjeravanje poruka (engl. *routing*), odnosno formiranje optimalne mrežne topologije. Ove dvije funkcije su glavne značajke ZigBee protokola. Mrežni sloj, kao i MAC, podržava određene sigurnosne mehanizme i adekvatni kriptirani prijenos podataka.

6.4 Aplikacijski sloj

Aplikacijski sloj zadužen je za ispravnu komunikaciju između aplikacija koje koriste ZigBee mrežu kao sredstvo komunikacije među čvorovima. Ovaj sloj kroji tablice uređaja, šalje poruke između povezanih uređaja, upravlja adresama grupa, ponovno sastavlja pakete i zadužen je za adekvatno pakiranje i prijenos podataka. Kao što je prikazano na slici 5., najviši je nivo i sastoji se od podsloja za aplikacijsku potporu ili APS-a. Također sadrži objekt ZigBee uređaja ZDO koji sadržava ZDO upravljački plan i AF aplikacijski okvir koji sadrži aplikacijske objekte koje definira proizvođač što je i jedina stvar koju definira proizvođač.

6.4.1 Aplikacijski okvir

Aplikacijski okvir (AF) okruženje je u kojem gostuju aplikacijski objekti na ZigBee uređajima. Do 254 različitih aplikacijskih objekata može biti definirano i numerirano adresom od 1 do 254. Identifikator 0 rezerviran je za podatkovno sučelje ZDO, a 255 za emitiranje, dok raspon od 241 do 254 trenutno nije u upotrebi, ali možda će biti u budućnosti ako ZigBee savez to potvrdi. Green Power klaster, ako bude implementiran, koristit će identifikator 242.

Aplikacijski profili dogovoreni su formati poruke, tipovi poruka i obrade određenih akcija kako bi razvojnim programerima bilo lakše da se stvaraju interoperabilne, distribuirane aplikacije i aplikacijski entiteti za razne uređaje. Ti aplikacijski profili omogućuju slanje naredbe, zahtjeva i obradu naredbi i zahtjeva.

Klasteri su identificirani pomoću jedinstvenog identifikatora koji se asociraju s podacima koji ulaze i izlaze iz uređaja. Identifikatori klastera jedinstveni su unutar određenog aplikacijskog profila.

6.4.2 Objekt ZigBee uređaja

Objekt ZigBee uređaja (ZDO) protokol je koji predstavlja osnovni razred funkcionalnosti za pružanje sučelja između aplikacijskih objekata i podsloja za aplikacijsku podršku. Zadovoljava učestale zahtjeve svih aplikacija poput:

- Inicijalizacije podrazreda za programsku podršku (APS), mrežnog sloja (NWK) i davatelja sigurnosnih usluga od strane APSDE-a za enkripciju podataka.
- Prikupljanja konfiguracijskih informacija od krajnjih aplikacija kako bi utvrdio i implementirao otkrivanje aplikacijskih objekata drugih uređaja. Upravlja sigurnosnim mjerama, mrežnim postavkama i upravlja spajanjem dvaju uređaja.

ZDO predstavlja javno sučelje aplikacijskim objektima u aplikacijskom okviru (AF) za kontrolu uređaja i mrežne funkcije. Zadužen je za definiranje uloge uređaja kao koordinatora ili krajnjeg uređaja i identificira njihove nove ponuđene usluge. Zatim nastavlja s uspostavljanjem sigurnih veza s vanjskim uređajima i u skladu s tim odgovara na obvezujuće zahtjeve.

Otkrivanje uređaja proces je u kojem ZigBee uređaj može otkriti drugi ZigBee uređaj, a postoje dva oblika otkrivanja u odnosu na zahtjeve za otkrivanje: IEEE zahtjev adrese i NWK zahtjev adrese. IEEE zahtjev za adresom je emitiranje *unicast* zahtjeva prema pojedinačnom uređaju i pretpostavlja da je NWK adresa poznata. Zahtjev za NWK adresom šalje se svima, prema tome je *broadcast* i nosi poznate IEEE adrese kao korisne podatke (engl. *payload*).

Otkrivanje usluge proces je u kojem ostali uređaji otkrivaju mogućnosti određenog uređaja. Otkrivanje usluge može se postići izdavanjem upita za svaku adresu aplikacijskih objekata na datom uređaju ili značajku servisa za otkrivanje podudarnosti (*broadcast* ili *unicast*). Otkrivanje usluge definira i koristi razne opise kako bi se označile mogućnosti uređaja. Informacije o otkrivenim uslugama zatim mogu biti spremljene u predmemoriji u mreži. U slučaju da se ta usluga izvodi na određenom uređaju, ona može biti nedostupna za vrijeme otkrivanja.

6.4.3 Podsloj za aplikacijsku potporu

Podsloj za aplikacijsku potporu, isto zvani podrazred za programsku podršku (APS), pruža sučelje između mrežnog (NWK) sloja i aplikacijskog (APL) sloja kroz generalni set usluga koje su korištene od strane ZDO-a i aplikacijskih objekata koje definira proizvođač. Usluge su definirane kroz dva entiteta:

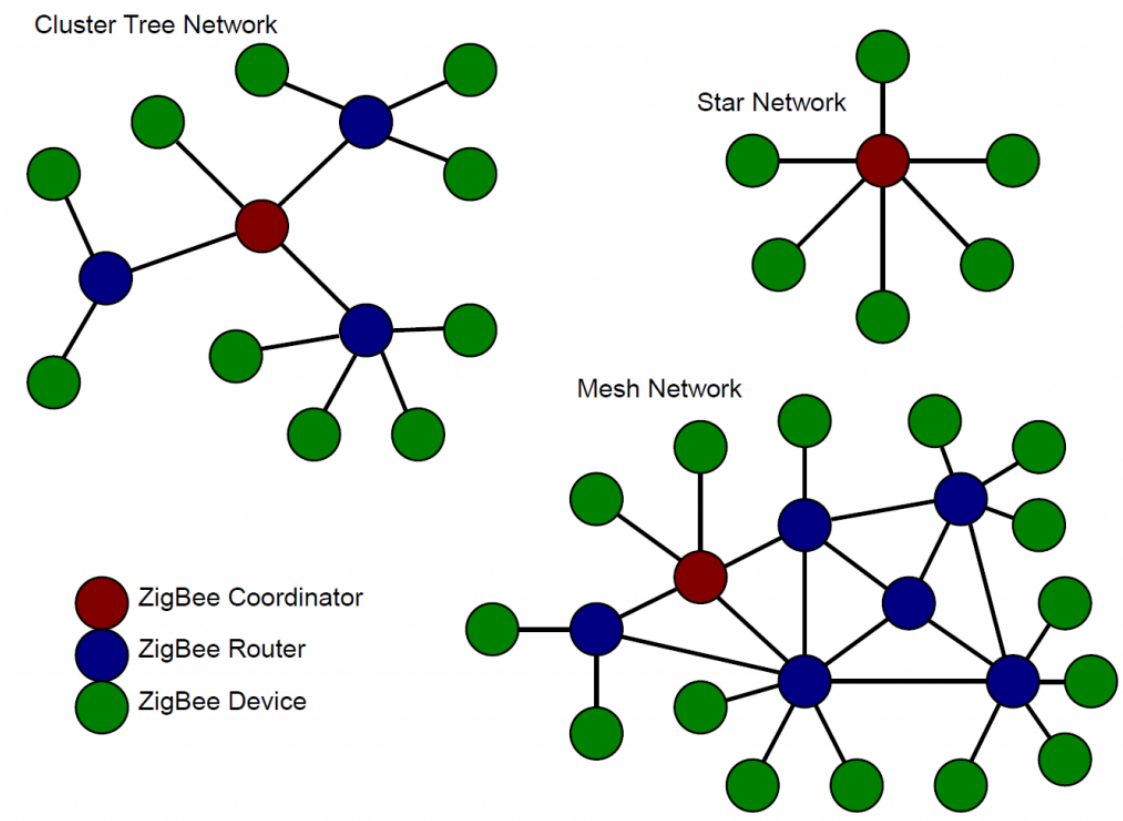
- APS podatkovni entitet (APSDE - *Application Support Sublayer Data Entity*) kroz APSDE uslugu pristupne točke (SAP - *Service Access Points*) (APSDE-SAP)
- APS upravljački entitet (APSME – *Application Support Sublayer Managament Entity*) kroz APSME uslugu.

APSDE pruža uslugu prijenosa podataka između dvaju ili više aplikacijskih entiteta na istoj mreži. APSME pruža različite usluge aplikacijskim objektima, uključujući sigurnosne servise i spajanje uređaja. Također, sadrži bazu podataka objekata kojima se upravlja, poznatu kao APS baza podataka (AIB – APS *information base*). Generalizira podatkovnu jedinicu protokola (PDU – *Protocol Dana Unit*) aplikacijske razine na način da uzme podatkovnu jedinicu, generira APS PDU, dakle podatkovnu jedinicu protokola podsloja za aplikacijsku potporu, te je nadogradi prikladnim protokolom koji dolazi iznad njega. APS spaja dva uređaja na način da APSDE može razmjenjivati podatke između njih, filtrira poruke na osnovu članstva adrese grupe, pruža pouzdan prijenos transakcija jer se, kao što je navedeno, nalazi iznad mrežnog (NWK) sloja, odbacuje dvostruke poruke te je posljednji cilj obaviti fragmentaciju na način da omogući segmentaciju i rastavljanje poruka većih od podataka korisne nosivosti koji stane u okvir mrežnog sloja.

6.5 Topologija ZigBee mreže

ZigBee mrežni sloj podržava topologije koje su podržane standardom IEEE 802.15.4 koji definira topologije za fizički sloj i sloj za pristup mediju, a nudi mrežastu topologiju (engl. *mesh*), topologiju zvijezde (engl. *star*), kombiniranu topologiju (engl. *cluster tree*) i topologiju drva (engl. *tree*), no ona nije podržana u ZigBee protokolu.

Koristi se asocijacija s hijerarhijom jer uređaj koji se pridružuje mreži ZigBee uređaja može biti isključivo ili usmjerivač ili krajnji uređaj. Koordinator je prvi i stvara mrežu, dok usmjerivači mogu povezati na sebe više uređaja.



Slika 6. Vrste ZigBee mrežnih topologija [13]

Topologija zvijezde sastoji se od koordinatora koji upravlja cijelom mrežom i nekoliko krajnjih čvorova. U ovoj topologiji krajnji čvor komunicira samo s koordinatorom. Bilo koji paket koji se šalje mora proći kroz koordinator. Nedostatak ove topologije je što operacija mreže ovisi isključivo o koordinatoru, a

činjenica da sav promet prolazi kroz koordinator, može biti posljedica zagušenja mreže. Drugi nedostatak je što nema drugog puta od izvora do destinacije. Prednost ove topologije je u tome što paketi jednostavno dolaze do svog odredišta kroz maksimalno dva skoka.

Topologija drva sastoji se od koordinatora koji je korijen drva, zatim se na njega spaja nekoliko usmjerivača i na kraju nekoliko krajnjih čvorova kao što je prikazano na slici. Funkcija koordinatora je proširiti doseg mreže. Krajnji čvorovi koji se spajaju na koordinator ili usmjerivač zovu se djeca. Krajnji čvorovi ne mogu imati djecu, već samo roditelji.

Mesh topologija, koja se također naziva engl. *peer-to-peer* mrežom, sastoji se od jednog koordinatora, nekoliko usmjerivača i krajnjih uređaja kao što je prikazano na slici 2.5. Karakteristike topologije *mesh* su:

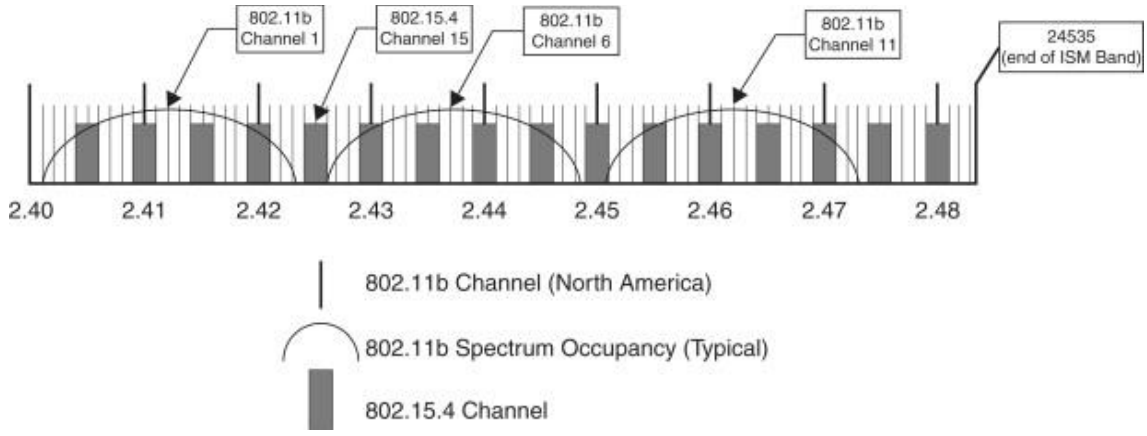
- podržava više skokova, prema tome paketi mogu napraviti više skokova kako bi dospjeli na svoje odredište
- doseg mreže može se povećati dodavanjem više uređaja u mrežu
- može eliminirati „mrtve zone“ jer je i drugi naziv za ovakvu vrstu topologije samoizlječiva i samoformirajuća, što znači da ako nestane putanja koja je prije postojala, čvor može naći drugu putanju gdje će poslati svoj paket
- uređaji mogu biti bliže i pritom trošiti manje energije za slanje poruka te je dodavanje ili izbacivanje uređaja iz mreže jednostavno.

Nedostaci su to što je usmjerivanje paketa kompleksnije i u usporedbi sa zvjezdanom topologijom zahtijeva više energije [10]. Takva vrsta mreže dobiva i nadimke poput samoizlječiva, samoformirajuća mreža koja koristi protokol AODV (engl. *Ad-hoc on-demand Distance Vector Routing protocol)* definiran kao RFC 3561 [11].

7. KOMUNIKACIJA ZIGBEE PROTOKOLA

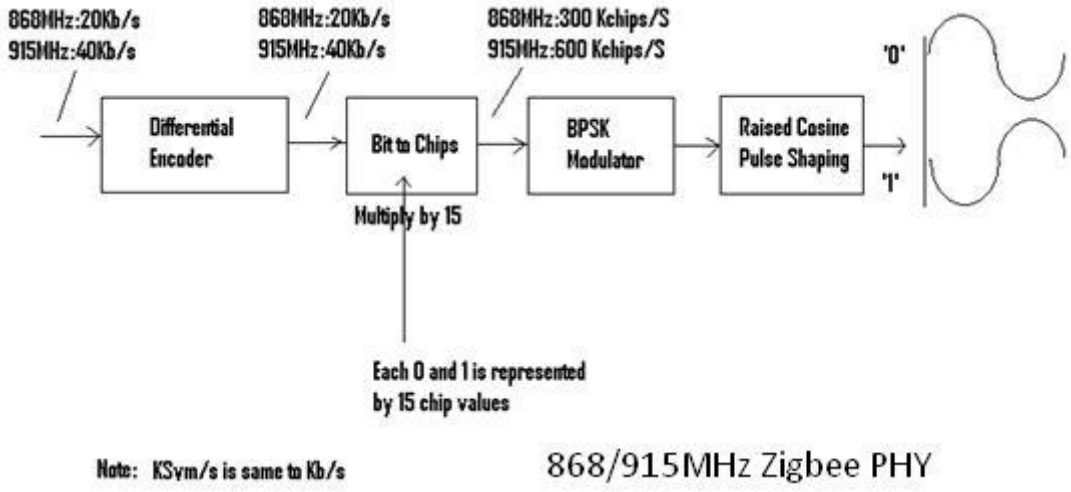
Kako bismo samostalno iskoristili ZigBee protokol na način da ga primjenjujemo u svojim DIY (engl. *Do It Yourself*) projektima, moramo znati na koji način ZigBee šalje poruke. U nadolazećem tekstu bit će navedeno kako ZigBee šalje poruke počevši od fizičkog sloja pa sloja za pristup mediju te će biti objašnjen mrežni sloj i naposljetku aplikacijski sloj. Na taj će način biti razumljivije kako programirati aplikacije za ZigBee uređaje.

7.1 Komunikacija podataka fizičkim slojem



Slika 7. ZigBee i WiFi kanali [12]

Jedna od zanimljivih činjenica o WiFiju i ZigBeeju je da WiFi obično koristi kanale 1, 6 ili 11 što znači da će mnogo ZigBee kanala biti slobodno, bez obzira na to koji kanal WiFi zauzme u datom trenutku. Kao što se vidi na slici 7., ZigBee (802.15.4) kanali 15, 20, 25 i 26 uvijek su bez smetnji i nisu u opoziciji s kanalima 1, 6 i 11 protokola standarda 802.11b, bez obzira na to koji se WiFi kanal koristi.



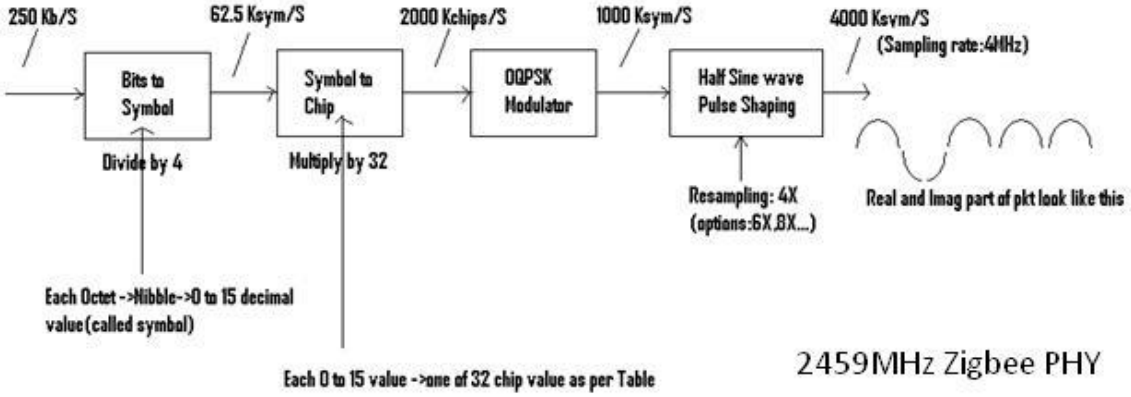
Slika 8. Modulacija fizičkog sloja 868/915 [13]

Slika 8. prikazuje na koji se način podaci moduliraju binarnom PSK modulacijom. Najprije ulaze u diferencijalni enkoder, zatim se dijele u komadiće (engl. *chips*), po njih 15. Nakon toga se komadići moduliraju u BPSK bloku i naposljetku se modulirani signal provodi kroz filter povišenih kosinusa i lanac koji izađe modulira se pomoću radijsko-frekvencijskog primopredajnika.

En = EX-OR od Rn i En-1

Rn su sirovi podaci koji se kodiraju, En su sukladni bitovi koji su kodirani, a En-1 su prošli diferencijalni bitovi koji su prošli operaciju digitalne algebre.

Kod demodulacije isti se postupak vrši obrnuto.



Slika 9. Modulacija fizičkog sloja 2450 [13]

Na slici 9. prikazana je modulacija fizičkog sloja 2.4 GHz koja počinje dijeljenjem okteta na dva dijela (engl. *nibbles*) koji se zovu simboli, dakle dijeli se bajt sa 4. Iz jednog bajta, odnosno okteta nastanu dva simbola. Svaki simbol je heksadecimalna znamenka, tj. predstavlja broj od nula do 15. Dalje se simboli dijele na komadiće na temelju tablice, a zatim ti komadići idu u OQPSK modulator gdje se moduliraju. Zatim prolaze kroz polusinusni filter koji oblikuje puls prije nego se pretvore u modulirani radioval. Kao i kod modulacije fizičkog sloja 868/915, demodulacija se vrši na isti način u drugom smjeru.

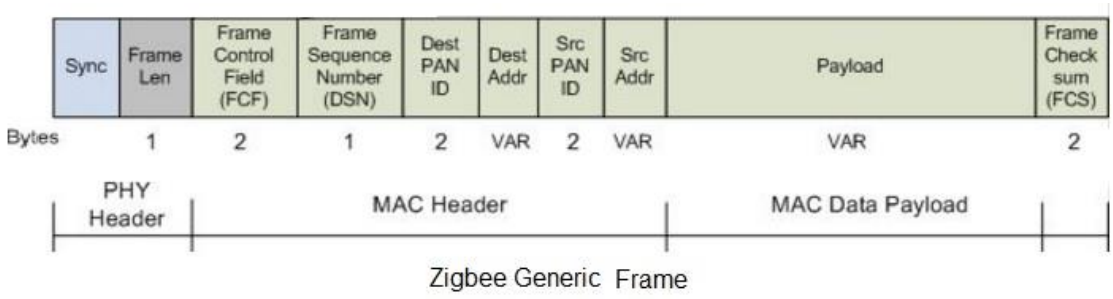
Octets:4	1	1		variable
Preamble	SFD	Frame length(7 bits)	reserved(1 bit)	PSDU
SHR		PHR		PHY payload

Slika 10. Struktura ZigBee PPDU paketa [13]

Jedinice podataka protokola koje se šalju fizičkim slojem jesu bitovi, no postoji i naziv fizičkog protokola koji se zove PPDU (engl. *Physical Protocol Dana Unit*), a sastoji se od zaglavlja za sinkronizaciju (SHR – engl. *Synchronisation Header*), zaglavlja fizičkog sloja (PHR – engl. *PHY Header*) i samih podataka korisne nosivosti (engl. *PHY Payload*). Dalje podjela slijedi tako da se SHR od ukupno pet okteta dijeli na uvodno polje (engl. *Preamble*) koje zauzima kapacitet četiri okteta, a obične su nule s ciljem da se označi paket. Unutar je još polje za podjelu uvodnog dijela i početak paketa (SFD - engl. *Start-of frame delimiter*). Zaglavlje fizičkog sloja PHR sastoji se od sedam bitova koji indiciraju dužinu paketa i jedan bit koji ima oznaku rezervirano. PHY okvir se ne dijeli. On ima korisnu nosivost i unutar njega ide paket MAC sloja.

7.2 Komunikacija podataka MAC slojem

Kao i svi mrežni uređaji, ZigBee također ima MAC adresu koja se naziva i IEEE adresa, duga adresa ili proširena adresa. Ona je 64-bitni broj koji jedinstveno identificira ovu tiskanu pločicu od svih ostalih ZigBee ploča u svijetu. Taj je broj dovoljno velik da omogući oko četiri milijarde ZigBee pločica. ZigBee vjeruje da će to biti dovoljno velik adresni prostor za doglednu budućnost. Prva 24 bita ove adrese sastoje se od jedinstvenog organizacijskog identifikatora (OUI). Donjih 40 bita upravlja OEM proizvođač ploča. Na primjer, sve Freescale razvojne pločice koriste OUI 0x0050c2. Ostatak bitova 0x37b001xxxx definira specifičnu ZigBee razvojnu pločicu.



Slika 11. ZigBee generičan okvir [13]

Ako bacimo pogled na pakete sloja za kontrolu pristupa mediju, vidimo da ima okvir za vrstu paketa (FCF - engl. *Frame Control Field*) od dva bajta u kojemu se može naći primjerice bajt koji izgleda poput „000…“ što znači da šaljemo paket odašiljača, slanjem bajta oblika „001…“ znači da ćemo poslati neke informacije, „011…“ su MAC naredbe kojima šaljemo neke naredbe za upravljanje, a „100…-111…“ su rezervirane za buduću primjenu. Ako neki paket nestane ili nije dobro poslan, postoji broj za provjeru reda za mjesto koje šaljemo (DSN – engl. *Destination Sequence Number*). Nakon toga slijede okviri za adresiranje: šalje se PAN identifikator (engl. *Destination PAN Identifier*) i prava adresa uređaja na koji želimo poslati (engl. *Destination address*). Isto tako šalju se podaci izvornog uređaja koji šalje pakete. Poslije adresnog polja stižu ponovno podaci korisne nosivosti (engl. *MAC Data payload*) u koje se pakiraju podaci višeg sloja. Na kraju stoji zaglavlje paketa za provjeru sekvence (engl. *Frame check sequence*) i

provjeru integriteta paketa. Ako neki bit nedostaje, rezultat algoritma pokazat će narušenje integriteta paketa i potom se može poslati zahtjev za ponovno slanje paketa.

7.3 Komunikacija podataka mrežnim slojem

Komunikacija mrežnog sloja uglavnom se vrti na AODV protokolu koji smo spomenuli prije. Spomenut ćemo da 802.15.4 protokol određuje dvije adrese, 16-bitnu mrežnu adresu i 64-bitnu adresu. 16-bitna mrežna adresa dodjeljuje se čvoru kada se spoji na mrežu, jedinstvena je svakom čvoru u mreži, nije statična i sklona je promjeni, pa prema tome uređaj zahtijeva novu adresu pod ovim uvjetima:

- Ako je došlo do problema u komunikaciji između uređaja i njegova roditelja, tada ZigBee čvor napušta mrežu i ponovo se spaja kako bi našao novog roditelja.
- Ako se vrsta uređaja promijeni iz vrste dijete u roditelj, odnosno krajnji čvor postane usmjerivač, isto vrijedi i za obrnutu situaciju.

ZigBee zahtijeva da se podaci šalju na 16-bitnu mrežnu adresu uređaja, stoga je važno znati 16-bitnu adresu prije slanja podataka.

Svaki čvor sadrži 64-bitnu adresu koja je jedinstvena i trajna. ZigBee aplikacijski sloj definira krajnje točke i identifikatore klastera koji su korišteni za adresiranje pojedine usluge ili aplikacije na uređaju. Krajnja je točka određeni zadatak koji aplikacija izvodi na uređaju, slično kao i TCP port. Svaki ZigBee uređaj može imati jednu ili više krajnjih točki. Identifikatori klastera slični su funkcijama ili akcijama na određenom uređaju. Oni se primjerice koriste za kontrolu svjetla, poput akcija naredbe „TurnLightOn“ za paljenje svjetla, „TurnLightOff" za gašenje svjetla, naredbe "DimLight" za promjenu razine svjetlosti itd. Tako da su svi paketi adresirani adresama uređaja i adresama aplikacijskog sloja, a mogu biti poslani kao *broadcast* ili *unicast*.

Broadcast u ZigBee protokolu namijenjen je za propagaciju poruke kroz cijelu mrežu tako da svi čvorovi prime poruku. Da bi se to postiglo, svi uređaji koji prime *broadcast* poruku ponovno odašilju isti paket tri puta.

Unicast odašiljanje u ZigBee komunikaciji oslanja se na 16-bitnu adresu iako nije trajna. Stoga je potrebno identificirati 16-bitnu adresu iz poznate 64-bitne adrese prije slanja podataka. Ova identifikacija uspijeva posebnim mrežnim protokolom za otkrivanje adrese, a već spomenuti AODV protokol služi za otkrivanje najbolje putanje, odnosno rute.

Prijenosom podataka oni se uvijek šalju na 16-bitnu mrežnu adresu odredišnog uređaja. Međutim, budući da je 64-bitna adresa jedinstvena za svaki uređaj i općenito je poznata, ZigBee uređaji moraju otkriti mrežnu adresu koja je dodijeljena određenom uređaju kada se pridružio PAN-u prije nego što počnu s prijenosom podataka.

Da bi to učinio, uređaj koji započinje prijenos šalje prijenos otkrivanja adrese emitirane kao *broadcast* po cijeloj mreži. Ovaj paket sadrži 64-bitnu adresu uređaja na koji inicijator treba poslati podatke. Uređaji koji primaju ovaj prijenos emitiranja provjeravaju odgovara li njihova 64-bitna adresa 64-bitnoj adresi sadržanoj u emitiranom *broadcast* prijenosu. Ako se adrese podudaraju, uređaj šalje paket odgovora inicijatoru pružajući mrežnu adresu uređaja s odgovarajućom 64-bitnom adresom. Kad se primi ovaj odgovor, inicijator tada može prenijeti podatke.

ZigBee koristi mrežno usmjeravanje za uspostavljanje rute između izvornog uređaja i odredišta. Mrežno usmjeravanje omogućuje podatkovnim paketima da prelaze više čvorova (skokova) u mreži za usmjeravanje podataka od izvora do odredišta. Ruteri i koordinatori mogu sudjelovati u uspostavljanju ruta između izvornih i odredišnih uređaja pomoću procesa koji se naziva otkrivanje rute. Postupak otkrivanja rute temelji se na protokolu AODV (*Ad-hoc On-demand Distance Vector routing*).

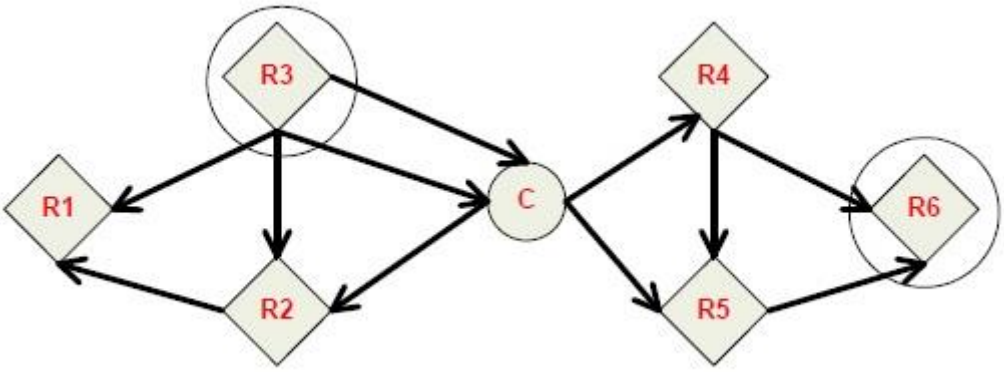
7.3.1 Traženje najbolje rute u ZigBee mreži

Usmjeravanje prema AODV protokolu postiže se pomoću tablica u svakom čvoru koje spremaju sljedeći skok (posrednički čvor između izvornog i odredišnog čvora) za odredišni čvor. Ako sljedeći skok nije poznat, mora se otkriti ruta da bi se pronašao put. Budući da se samo ograničeni broj ruta može pohraniti na usmjerivač, otkrivanje ruta češće će se odvijati na velikoj mreži s komunikacijom između mnogo različitih čvorova.

Čvor	Odredišna adresa	Adresa idućeg skoka
R3	Router 6	Koordinator
C	Router 6	Router 5
R5	Router 6	Router 6

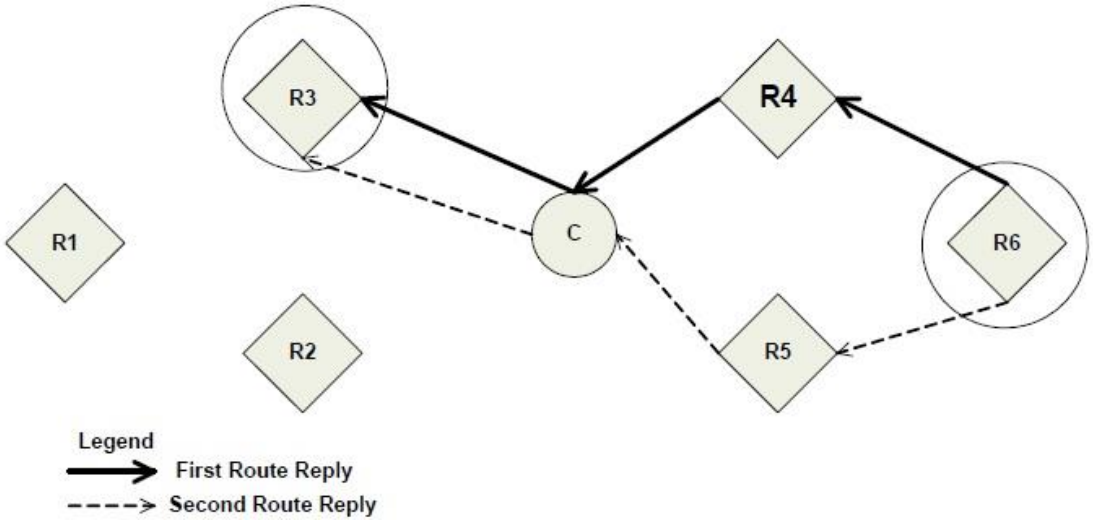
Tablica 1. Skokovi kroz ZigBee mrežu [13]

Kada izvorni čvor mora otkriti rutu do odredišnog čvora, šalje naredbu zahtjeva za emitiranu rutu. Naredba zahtjeva rute sadrži izvornu mrežnu adresu, odredišnu mrežnu adresu i cijenu puta (metrika za mjerenje kvalitete rute). Kako se naredba zahtjeva rute širi putem mreže, tako svaki čvor koji ponovno emitira *broadcast* poruku, ažurira polje cijene puta i stvara privremeni unos u svojoj tablici otkrivanja rute.



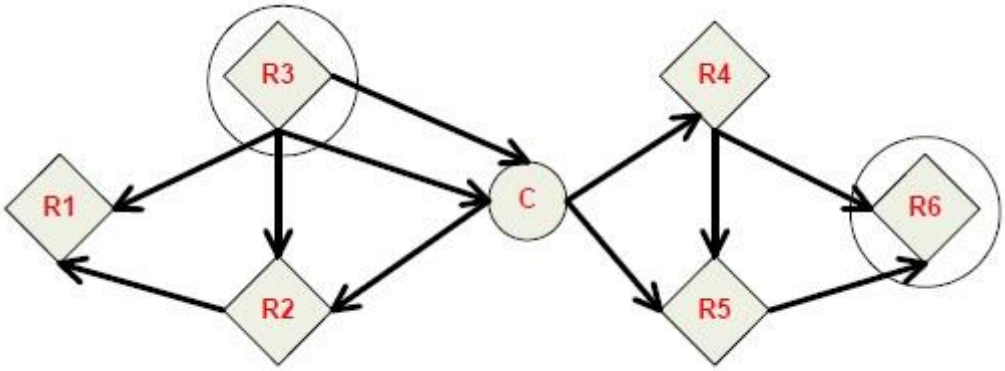
Slika 12. Primjer emitiranja broadcast zahtjeva za pronalaženje rute od R3 do R6

Kad odredišni čvor primi zahtjev za rutu, uspoređuje cijenu s prethodno primljenim naredbama zahtjeva rute. Ako je cijena puta pohranjena u zahtjevu rute bolja od bilo koje prethodno primljene, odredišni čvor poslat će paket odgovora rute čvoru koji je pokrenuo zahtjev rute. Srednji čvorovi primaju i prosljeđuju paket odgovora rute izvornom čvoru (čvor koji je podnio zahtjev za rutu).



Slika 13. Slanje odgovora od strane R6 prema R4 za pronalaženje rute

Ovdje R6 može poslati više odgovora ako identificira bolju rutu. ZigBee uključuje pakete potvrde na slojevima MAC i sloju aplikacijske podrške (APS). Kada se podaci prenose na udaljeni uređaj, može prijeći više skokova do odredišta. Kako se podaci prenose s jednog čvora na susjeda, paket potvrde (Ack) prenosi se u suprotnom smjeru kako bi označio da je prijenos uspješno primljen. Ako „Ack“ nije primljen, uređaj za odašiljanje ponovno će poslati podatke, do četiri puta. Ovaj „Ack“ naziva se potvrda Mac sloja.



Slika 14. Slanje „Ack“ odgovora natrag

Osim toga, uređaj koji je započeo prijenos, očekuje primitak paketa potvrde (Ack) od odredišnog uređaja. Ovaj „Ack“ će prijeći isti put kojim su prešli podaci, ali u suprotnom smjeru. Ako inicijator ne uspije primiti ovaj „Ack“, ponovno će poslati podatke, najviše dva puta dok se „Ack“ ne primi. Ovaj „Ack“ naziva se potvrda ZigBee APS sloja.

7.3.2 Formiranje ZigBee mreže

Koordinator traži odgovarajući RF kanal koji je upotrebljiv i ne ometa frekvencije bežične LAN mreže u upotrebi. To se radi na svih 16 kanala. Naziva se i energetsko skeniranje.

Koordinator pokreće mrežu dodjelom PAN ID-a mreži. Dodjela se vrši na dva načina. Ručno (unaprijed konfigurirano) i dinamičko (dobiveno provjerom drugih PAN ID-ova mreža koje su već u operaciji u blizini tako da PAN ID ne dolazi u sukob s drugim mrežama). Ovdje koordinator također sebi dodjeljuje mrežnu adresu, tj. 0x0000.

Sada koordinator dovršava svoju konfiguraciju i spreman je prihvatiti upite sa zahtjevima za pridruživanje mreži od usmjerivača i krajnjih uređaja koji se žele pridružiti PAN-u.

Osim gore navedenog, koordinator (C) šalje okvir zahtjeva za emitiranje signala na preostalom mirnom kanalu. To se također naziva *beacon scan* ili PAN *scan* što prevedeno znači skeniranje stanice, odnosno osobne mreže. Ovime koordinator prima PAN ID usmjerivača (R) i krajnjih uređaja (E) prisutnih u blizini. Također, dolazi do znanja dopušta li R/E pridruživanje ili ne. Sada se R/E može pridružiti slanjem zahtjeva za pridruživanjem C. C će odgovoriti odgovorom za spajanje. I na taj će način uređaji obaviti spajanje.

7.3.3 Pridruživanje ZigBee mreži

Ispitajmo kako se usmjerivač ili krajnji uređaj pridružuje ZigBee mreži u sklopu ZigBee vodiča. ZigBee mreži mogu se pridružiti na dva načina, tj. MAC pridruživanjem i ponovnim pridruživanjem mreži.

Prvi je implementiran uređajem koji se nalazi ispod MAC sloja, a drugi je implementiran mrežnim slojem unatoč tome što se naziv također može koristiti za pridruživanje mreži prvi put.

MAC povezivanje može se izvesti između C i R/E ili R i E ili R i drugih R.

Pretpostavimo da je koordinator (C) već uspostavio PAN mrežu. Stoga je sljedeći korak za R ili E da saznamo dopušta li C pridruživanje ili ne. Tako rade PAN skeniranje ili šalju okvir zahtjeva za stanicu (engl. *beacon*).

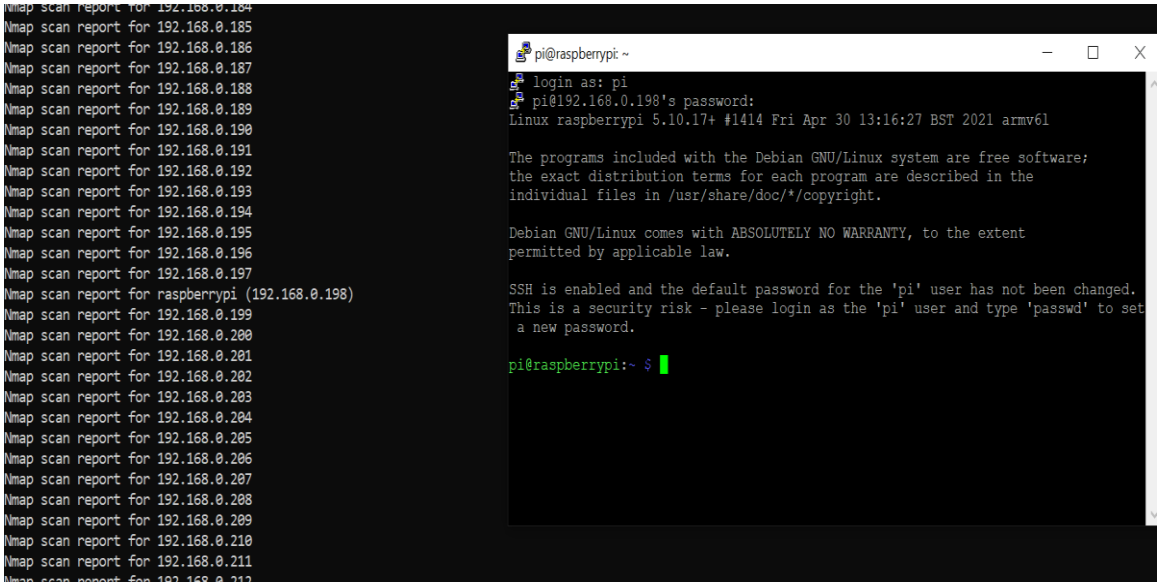
Nakon što saznaju da se mogu pridružiti mreži, poslat će okvir zahtjeva za pridruživanjem i pridružit će se mreži čim dobiju odgovor stanice.

Kao što je spomenuto, hoće li C ili R dopustiti pridruživanje novog uređaja ovisi o dvama glavnim čimbenicima:

- o dozvoljavanju pridruživanja atributu
- o broju djece, odnosno krajnjih uređaja koje već ima.

8. RASPBERRY PI

Kao što je već navedeno, cilj je opis izvedbe mreže između kućnih uređaja u pametnom domu pomoću ZigBee protokola, a ostvaruje se konfiguriranim Raspberry Pi-jem koji će se koristiti kao usmjernik i modul za ZigBee koji se spaja pomoću USB-a na Raspberry Pi i instalacije Homeassistant aplikacije.



Slika 15. Pristupanje Raspbian sustavu preko SSH-a putem Putty alata

Nakon brzog skeniranja alatom nmap možemo saznati IP adresu Raspberry uređaja na lokalnoj mreži. Nakon toga možemo se ulogirati u Raspberry Pi putem Putty alata preko SSH-a na portu 22. Pošto sve nove instalacije sustava Raspbian inicijalno imaju iste login podatke, vjerodajnica za Raspbian OS inicijalno su, korisničko ime: „*pi*“ i lozinka: „*raspberry*“. Zatim imamo pristup terminalu preko SSH-a i možemo za početak nadograditi sustav što je i preporučljivo nakon prvog logina postaviti lokalnu statičnu IP adresu zbog lakše prijave i promjena lozinke naredbom *sudo apt update && apt upgrade –y* što će provjeriti javne repozitorije da li ima koji paket za unaprijediti, nakon čega će se skinuti i instalirati. Tek tada konačno možemo instalirate ostale dodatke i dodatne pakete.

9. HOMEASSISTANT

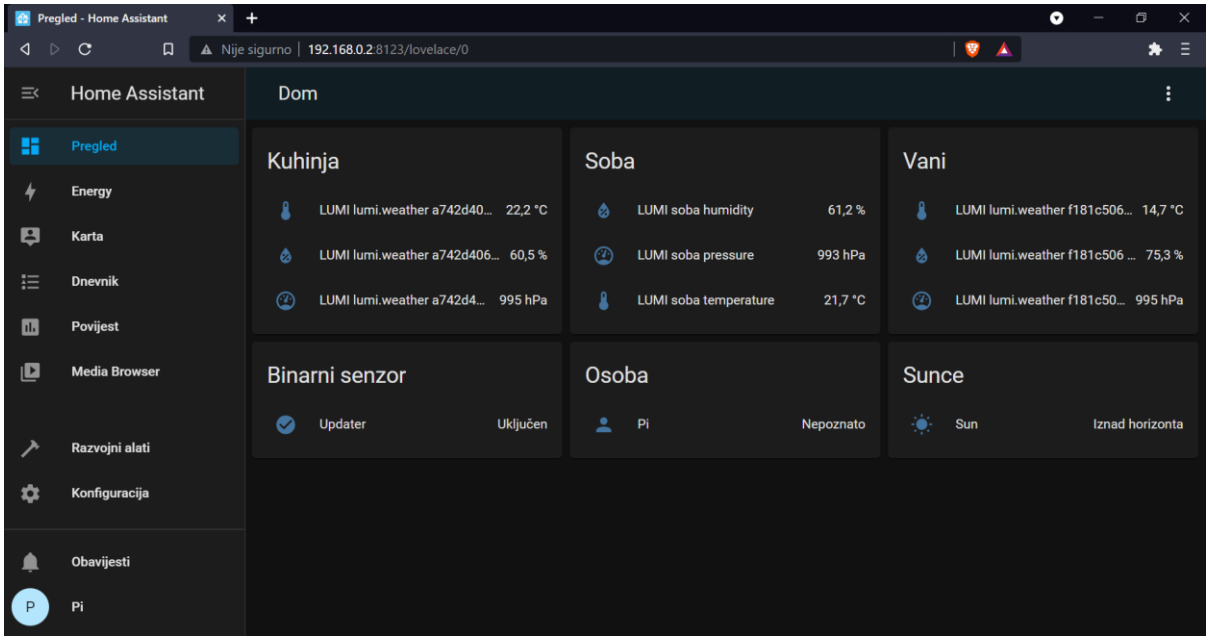
Homeassistant, skraćeno Hass, aplikacija je koja radi na više od 1000 različitih uređaja, možemo ju instalirati na virtualne mašine, servere lokalnih mreža, poput Raspberry Pi-ja. Omogućuje potpunu automatizaciju sustava i integraciju svih uređaja u pametnom domu, stoga se sve značajke svih vrsta protokola mogu iskoristiti. Podržava dodavanje softverskih dodataka (engl. *Add-ons*) kao što su *Ad Guard, Spotify Connect, Pi-Hole*… Postoje algoritmi za uređaje u domu koji štede energiju i postoji aplikacija za pametni telefon. Svi podaci ostaju na lokalnom serveru pa nema potrebe za *cloud* servisima te se time i uvelike smanjuje rizik od neželjenih potencijalnih opasnosti koje vrebaju s interneta.

Homeassistant aplikacijsku podršku možemo instalirati na tri načina:

- U kontejner (engl. *container*), kao primjerice *Docker*. *Docker* je tehnologija za kreiranje softverskih kontejnera što su paketi pojedinačnih aplikacija koji sadrže sve neophodno za pokretanje i izvršavanje. Na jednom serveru može se izvršavati više kontejnera istovremeno, ali sve mora pokretati isti operativni sistem.
- Kao sliku koja vrti Linux distribuciju isključivo Hass sustava.
- Kao Homeassistant jezgru koja se instalira i izvodi u virtualnom okruženju Pythona jer je pisan u tom jeziku.

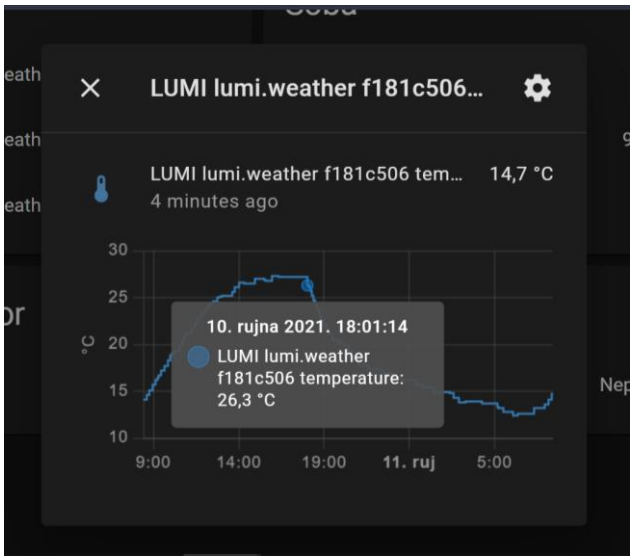
Za Raspberry Pi, osobito starije verzije sa slabijim karakteristika, najbolje je instalirati Hass sustav jer je minimalan i pisani kod isključivo za optimizaciju za aplikaciju koja će se izvoditi na njemu, a to je Homeassistant. Druga po redu od boljih opcija svakako bi bila instalacije jezgre koja, iako se izvodi u pozadini preko Python virtualnog okruženja, svakako nudi bolje performanse zbog sukladnosti programskog jezika. Ostale opcije nude nešto slabije, no ne neoprostive performanse zbog prevođenja procesa u virtualnim okruženjima. Nakon instalacije Homeassistanta slijedi konfiguracija ostalih uređaja umreženog sustava (razni senzori, svjetiljke, utičnice itd.). Spajanje na Raspberry Pi iz bilo koje daljinske mreže možemo ostvariti instalacijom programskog dodatka PiVPN na Raspberry i, naravno, postavljanjem statične IP adrese i/ili dinamičnom IP

adresom i DDNS-om. Na taj način možemo ostvariti virtualnu privatnu mrežu i spajati se s bilo kojeg mjesta na kojem imamo pristup internetu.



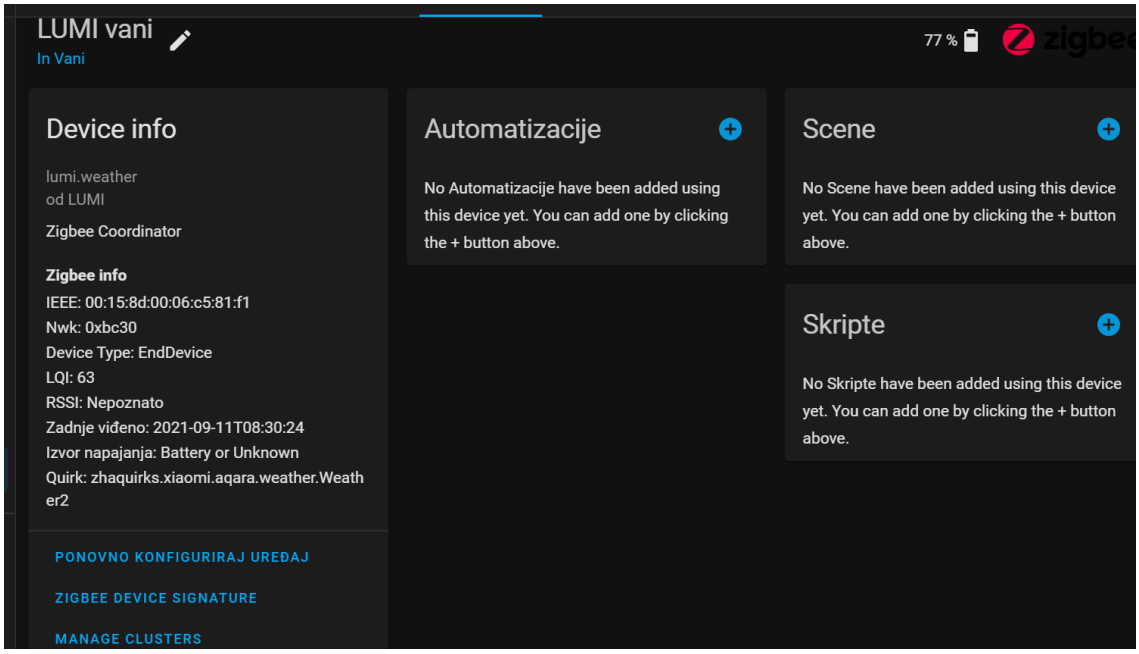
Slika 16. Izgled sučelja Homeassistant

Na slici 16. nalazi se primjer kako izgleda sučelje Homeassistanta. Nalazi se na adresi 192.168.0.2. Adresa Raspberry Pi računala i port Homeassistant servisa je :8123. Prijavljen je korisnik Pi, a u sučelju se pojavljuju tri senzora za različite položaje koji se aktiviraju isključivo kod promjene temperature što se i vidi na slici 17.



Slika 17. Primjer kako ZigBee senzor očitava temperaturu

Graf na slici 17. prikazuje povijest temperature tijekom 24 sata. Pomakom kursora vidi se svaka točka kada je ZigBee senzor zabilježio temperaturu. Ispod naslova uređaja također vidimo da je ZigBee uređaj u ovom slučaju posljednje bio aktivan i zabilježio temperaturu prije četiri minute što nam govori da ZigBee uređaj javlja temperaturu samo kod promjene temperature i time štedi energiju.



Slika 18. Primjer kako ZigBee senzora koji se nalazi vani

Svu teoriju koju smo prošli u ovom radu možemo vidjeti na slici broj 18. Jasno se vide informacije o uređaju poput naziva uređaja: LUMI Vani, Info: lumi.Weather, vrsta uređaja: krajnji čvor, IEEE ili MAC adresa: 00:15:8d:00:06:c5:81:f1. LQI (engl. *Link Quality Indicator*) mjeri kvalitetu veze na MAC sloju: 63, postotak baterije kada je uređaj zadnje poslao poruku, tj. komunicirao s nama i kakve skripte scenarije i automatizacije postoje za njega.

9.1 Filozofija otvorenog koda

Homeassistant kućna je automatizacija otvorenog koda koja lokalnu kontrolu i privatnost stavlja na prvo mjesto. Pokreće ga svjetska zajednica majstora i entuzijasta "uradi sam". Kod Homeassistant repozitorija može se naći na Githubu na kojem radi veliko društvo stručnjaka i zbog kojeg se nadograđuju značajke, kompatibilnost i svi aspekti uključujući sigurnost. Na primjer, kad se pronađe neki sigurnosni propust ili nedostatak, a često se otkrije brzo zbog količine ljudi koja koristi i razvija Homeassistant, još se brže taj propust ili nedostatak riješi.

10. SIGURNOST

Svaki umreženi uređaj stvara sigurnosni rizik i potencijalna je meta za maliciozne napadače. Također, postoji pogrešna koncepcija pučanstva da se takvi uređaji lako probijaju i da su često meta napadačima. Ipak, strah je opravdan i jasan jer su uređaji u pametnom domu bliski našoj privatnosti i utječu na funkcije koje se događaju u mjestu gdje stanujemo te nikako ne bi smjele biti podložne napadima.

Za početak treba spomenuti da prosječni građanin neće imati isti rizik kao i osoba s primamljivim motivima. U zadnjoj objavi kompanije koja proizvodi popularni antivirusni softver Avast navedeno je da je oko 40 % uređaja na mreži podložno napadima na daljinu s interneta, od čega su velika većina uređaja printeri i usmjerivači. Na to najčešće ne pomislimo kad je riječ o pametnom domu i sigurnosti pametnih svjetala, brava, utičnica itd.

Stoga smatram da većina ljudi nema razloga za strah što se tiče sigurnosti mreže pametnog doma. Ono što možemo učiniti kako bi se poboljšala sigurnost od napadača, je unaprjeđivanje fiksnog programa (engl. *firmware*) usmjerivača i izbjegavanje korištenja lozinki koje su slične čestim riječima (*password*, lozinka, brojevi od 0 do 9 ili obrnuto, imena, prezimena itd.). Uz to, preporučljivo je držati osjetljive i privatne informacije na zasebnoj VLAN mreži od one na kojoj se nalaze IoT internet stvari (engl. *Internet of Things*), uređaji, a ako se spajamo na kućnu mrežu s javnog interneta, također bi trebalo koristiti VPN pa na taj način osigurati dodatnu enkripciju i još jednu razinu sigurnosti.

Što se tiče ZgiBee uređaja, poruke su obično kriptirane s AES enkripcijom i 128-bitnim ključem. Ranjivost tih uređaja, osobito jeftinijih, leži u prikupljanju informacija koje periodički šalju svojim serverima proizvođača ako se koristi komercijalni usmjerivač pametnih uređaja. Osim toga, često izbace ažuriranja koja se odvijaju automatski bez znanja korisnika što je opet jedan od dodatnih prozora za provalnika. Sigurnost ZigBee uređaja leži u tome što je drugačiji način adresiranja tih uređaja i ne koriste konvencionalni TCP/IP model i metode. Brzina prijenosa podataka sporija je pa bi, prema tome, provalnik trebao imati i mnogo strpljenja.

11. ZAKLJUČAK

Ovim završnim radom iskazali smo kakvi sustavi za umrežavanje uređaja u pametnom domu postoje i na koji bi se način trebali umrežavati, a prikazano je i koje su prednosti i nedostaci takvih sustava. Prednost je što je pristupačno više-manje svima te nudi udobnost korisniku u njegovu pametnom domu s jednim zajedničkim sučeljem preko kojeg se može pristupiti, automatizirati i upravljati svim uređajima. Takva implementacija ne predstavlja veliki sigurnosni rizik i vrlo je korisna, osobito za napredne korisnike koji znaju iskoristiti svoje znanje u praksi.

Problem i nedostaci su upravo u tome što kod svake zamjene uređaja pametni dom iziskuje strpljenje, znanje, volju za učenjem, osobito kod zahtjevnijih konfiguracija unutar Linux sustava u slučaju da nešto pođe po zlu, ako se nešto izbriše ili jednostavno ako zahtijeva unaprjeđenje neke aplikacije, servisa ili okruženja. Samo kod zamjene ili dodavanja uređaja potrebna je nova konfiguracija što opet od prosječnog korisnika iziskuje vremena i strpljenje.

Ono što je dojmljivo je da takvi sustavi postoje, moguće ih je umrežiti i nude ogroman broj kombinacija za automatizaciju, nadziranje i upravljanje. Dostupno je svima preko mreže svih mreža, a Homeassistant, kao i Linux i ostali projekti otvorenog koda imaju čini se beskrajnu, neumoljivu potporu. Dojmljiva je snaga otvorenog koda.

12. POPIS LITERATURE

[1] Applications, Systems and Methods in Smart Home Technology: A Review (January 2010), University of San Agustinm, (11. 7. 2021.)

[2] Preville, Cherie (26 Aug 2013). "Control Your Castle: The Latest in HVAC Home Automation". ACHRNews, (11. 7. 2021)

[3] Tom's Home Automation Webpage, http://www.laureanno.com/, (11. 7. 2021.)

[4] Remote UI, https://www.nabucasa.com/config/remote, (10. 9. 2021)

[5] Common requirements for Carrier Grade NATs (CGNs) draft-ietf-behave-lsn-requirements-10, https://datatracker.ietf.org/doc/html/draft-ietf-behave-lsn-requirements, (10. 9. 2021.)

[6] Drew Gislason, Zigbee Wireless Networking, 21 August 2008, Newnes

[7] IEEE 802.15.4-2020 - IEEE Standard for Low-Rate Wireless Networks, https://standards.ieee.org/standard/802_15_4-2020.html, (11. 7. 2021.)

[8] ZigBee Specifiation, (May 2015), https://zigbeealliance.org/wp-content/uploads/2019/12/docs-05-3474-21-0csg-zigbee-specification.pdf, (12. 7. 2021.)

[9] What is ZigBee Technology and How it works, https://www.electricaltechnology.org/2017/09/zigbee-technology-wireless-networking-system.html, (11. 9. 2021.)

[10] Introduction to the ZigBee Wireless Sensor and Control Network, ZigBee Topologies, (2.12.2021.), InformIT, (11. 9. 2021.)

[11] Ad hoc On-Demand Distance Vector (AODV) Routing, (June 2003.), https://www.ietf.org/rfc/rfc3561.txt, (11. 9. 2021)

[12] ZigBee Gatways, ZigBee Wireless Networking, (2008.), https://www.sciencedirect.com/topics/engineering/zigbee-protocol, (11. 9. 2021.)

[13] Tutorial on ZigBee protocol basics, https://www.rfwireless-world.com/Tutorials/Zigbee_tutorial.html, (11. 9. 2021.)