Academia Oamenilor de Știință
din România

Universitatea Politehnica Timișoara

COMPETIȚIA DE PROIECTE DE CERCETARE A ACADEMIEI OAMENILOR DE ȘTIINȚĂ DIN ROMÂNIA DESTINATĂ TINERILOR CERCETĂTORI
"AOSR-TEAMS" EDIȚIA 2022-2023

RAPORT INTERMEDIAR DE ACTIVITATE

Titlul proiectului:
Digitalizarea mărimilor electrice prin dezvoltarea unui dispozitiv de monitorizare a consumatorilor casnici, în vederea analizei și îmbunătățirii consumului de energie electrică.

Echipa de cercetare:
Conf.dr.ing. Attila SIMO - coordonator
Asist.drd.ing. Adrian MARTIN - membru
Drd.ing. Loredana PAVEN - membru

Data: 30.07.2022

1. Obiectivul proiectului și importanța acestuia

Strategia energetică a Uniunii Europene stabilește prioritățile electroenergetice pentru următorii ani și prezintă măsurile care trebuie luate pentru a face față provocărilor legate de necesitatea reducerii consumului de energie electrică, de realizare a unei piețe echilibrate, în care să se garanteze furnizarea sigură a energiei electrice la preturi competitive. Comisia Europeană a stabilit că țările membre vor promova adoptarea tehnologiilor și inovării pentru rețelele inteligente (smart grids), contorizări inteligente (smart metering) stocarea energiei electrice și parteneriatele în proiectele de localități inteligente.

Dezvoltarea rețelelor electrice inteligente constituie o sarcină extrem de dificilă și de mare răspundere, în special dacă se ține cont de costul investițiilor în acest domeniu, de efectele pe termen lung și de implicațiile legate de protecția mediului. Scopul dezvoltării acestor rețele inteligente este de a asigura o dezvoltare coordonată a unui sistem fiabil, eficient și economic de distribuție a energiei electrice în beneficiul pe termen lung al utilizatorilor (operatori de distribuție, producători, consumatori).

Un prim pas, foarte important în această direcție, este digitizarea mărimilor electrice de interes, pentru a permite utilizatorilor casnici vizualizarea și analiza acestora, în vederea aducerii unor îmbunătățiri. În contextul actual, în care energia electrică s-a scumpit foarte mult în ultima perioadă, necesitatea unor dispozitive de monitorizare, accesibile ca și preț, pentru urmărirea consumului de energie electrică, este tot mai evidentă. Digitizarea este o procedură prin care datele în format analog sunt convertite în format electronic, creând practic o imagine digitală sau formă digitală a unui semnal, obiect, fotografie, material audio etc. În zilele noastre, digitizarea datelor ia forma cifrelor binare, fiind procesate de un computer sau prin alte proceduri. Mai specific, este conversia unui material din sursă analog într-o formă numerică. Digitizarea este destul de importantă pentru procesarea informației, stocare, transmisie, pentru că permite informației să fie coagulată. Permite totodată datelor să fie obținute și distribuite, propagate fără a fi reduse și să fie transpuse în formate noi când este necesar. Digitizarea este metoda cea mai favorabilă pentru stocarea informației pentru persoane sau organizații de oriunde din lume. Procedura este similară compromisului dintre un obiect și dispozitivul de fotografiere astfel încât reprezentarea sursei finale să fie cât mai aproape de realitate. Avantajul acestei proceduri stă în viteza și precizia cu care informația este transmisă, fără a fi degradată în comparație cu forma analog. Digitizarea se face în doi pași: discretizare și cuantizare.

Tehnologiile „fără fir” non-celulare nu sunt ideale pentru a conecta dispozitive cu un consum de energie redusă, distribuite pe zone geografice mari, deoarece raza de acțiune a acestor tehnologii este limitată la câteva sute de metri în cel mai bun caz. Prin urmare, dispozitivele nu pot fi instalate sau mutate în mod arbitrar oriunde, ceea ce este o cerință pentru multe aplicații pentru orașe inteligente, transport și logistică și monitorizarea faunei sălbatice etc. Rețelele WLAN clasice, pe de altă parte, se caracterizează prin zone de acoperire mai scurte și un consum mai mare de energie. Gama acestor tehnologii este extinsă utilizând o desfășurare densă de dispozitive și gateway-uri conectate utilizând rețele de tip multihop.

Tehnologiile Low Power Wide Area (LPWA) oferă seturi unice de caracteristici, inclusiv conectivitate pe suprafață largă pentru dispozitive cu putere redusă și cu rată redusă de date, care nu sunt furnizate de tehnologiile wireless clasice. Rețelele LPWA sunt unice, deoarece fac compromisuri diferite față de tehnologiile tradiționale predominante în peisajul IoT, cum ar fi rețelele fără fir cu rază scurtă de acțiune (Zig-Bee, Bluetooth, Z-Wave), rețelele locale fără fir vechi (WLAN) și rețelele celulare. (GSM, LTE) etc. Cu o rază de acțiune de la câțiva până la zeci de kilometri și o durată de viață a bateriei de zece ani și mai mult, tehnologiile LPWA sunt promițătoare pentru Internet cu consum redus de energie, costuri reduse și debit redus. Aceste caracteristici permit dispozitivelor să acopere zone geografice mari, astfel

încât dispozitivele IoT și M2M conectate prin tehnologiile LPWA pot fi pornite oriunde și oricând pentru a detecta și a interacționa cu mediul lor.

Datorită existenței rețelelor LPWA, IoT este și mai interesant. LPWA reprezintă o nouă paradigmă de comunicare, care va completa tehnologiile tradiționale celulare și wireless pe rază scurtă de acțiune în abordarea diverselor cerințe ale aplicațiilor IoT. IoT promite să schimbe modul în care trăim și lucrăm. IoT ne-ar putea ajuta să depășim provocările globale de top din cauza crizei energetice, epuizării resurselor etc. Pentru a realiza această viziune, „lucrurile" trebuie să-și simtă mediul, să împărtășească aceste informații între ei, precum și cu noi pentru a oferi o decizie inteligentă.

Merită clarificat faptul că tehnologiile LPWA realizează o rază lungă de funcționare și un consum de energie redusă în detrimentul ratei scăzute de date (de obicei, în ordine de zeci de kilobiți pe secundă) și a unei latențe mai mari (de obicei, în ordine de secunde sau minute). Prin urmare, este clar că tehnologiile LPWA nu sunt menite să abordeze fiecare caz de utilizare IoT. Mai exact, tehnologiile LPWA sunt luate în considerare pentru acele cazuri de utilizare care sunt tolerante la întârziere, nu au nevoie de rate mari de date și necesită, de obicei, un consum redus de energie și un cost redus.

Pe baza celor menționate, tematica proiectului se încadrează în preocupările actuale din domeniul dezvoltării digitale a societății dar și în domeniul ingineriei energetice. Preocupările sporite din acest domeniu sunt reflectate și de numărul mare de publicații din literatura de specialitate, care încearcă să soluționeze problemele conexe atât prin metode clasice cât și prin utilizarea tehnicilor moderne.

În acest context, obiectivul principal al proiectului se referă la dezvoltarea unui dispozitiv de monitorizare destinat măsurării mărimilor electrice în curent alternativ, în vederea îmbunătățirii consumului de energie electrică la consumatori casnici, utilizând tehnologii noi, cum ar fi tehnologia Low Power Wide Area (LPWA), pentru transmiterea datelor la distanțe mari (ordinul km) și tehnologii clasice, deja consacrate, cum ar fi tehnologia WiFi, pentru transmiterea datelor la distanțe mai mici (ordinul sute de metri). Se încearcă dezvoltarea unui astfel de dispozitiv la un preț accesibil și pentru consumatorii casnici, pentru a facilita accesul la date, permițând analiza acestora și ulterior îmbunătățirea consumului de energie electrică, unde cere situația. De asemenea, un alt aspect important este flexibilitatea dispozitivului din discuție, din punct de vedere hardware. Dispozitivul trebuie să fie de tip "plug and play" și să permită mutarea sa de la un consumator la altul rapid și ușor.

Dispozitivele actuale din comerț au următoarele dezavantaje, în momentul de față, în comparație cu cel propus: prețul de achiziție mai ridicat, sunt fixe,

Rezultatele obținute vor fi valorificate în cadrul unor reviste de largă circulație internațională cu factori de impact semnificativi și în cadrul unor lucrări la conferințe internaționale de prestigiu.

Elementele de dificultate sunt legate de următoarele aspecte:

- construcția elementelor hardware care trebuie adaptate utilizării în sectorul energiei electrice (senzori, antene, elemente de conectică);
- compatibilizarea acesteia cu echipamentele care există deja implementate (acolo unde este cazul) în sensul de a comunica și a prelua / transmite date;

Aceste aspecte urmează să fie abordate printr-o cooperare strânsă între membrii echipei de cercetare și agenții economici, aceștia din urmă având rolul de a furniza echipamentele "brute" și de a colabora cu membrii echipei în direcția soluționării problemelor legate de compatibilizare.

2. Rezultate intermediare

În această etapă a proiectului, echipa de cercetare, a încercat să identifice cerințele pe care să le îndeplinească dispozitivul de monitorizare în vederea creionării arhitecturii acestuia și pentru identificarea componentelor hardware, pentru construcția prototipului.

Dispozitivul de monitorizare mărimi electrice va furniza următoarele valori:

- frecvențe rețelei electrice
- tensiunea electrică
- intensitatea curentului electric
- factor de putere
- puterile aparentă, activă, reactivă
- energiile activă și reactivă

Pentru transmiterea datelor s-au studiat și e vor încerca următoarele tehnologii:

2.1. TEHNOLGIA DE COMUNICAȚIE WI-FI

Wi-Fi este numele obișnuit al unei tehnologii wireless populare folosită în rețelistică, telefoane mobile, jocuri video și altele, tehnologie suportata de aproape toate PC-urile moderne și majoritatea consolelor de jocuri. Wi-Fi se bazează pe standardele IEEE 802.11 și utilizează mai multe tipuri de tehnologii bazate pe unde radio, care au dus la succesul în fața unor competitori ca Bluetooth.

Începutul tehnologiei cu spectru larg poate fi datat în 1985, când FCC(Comisia Federală pentru Comunicații SUA) a făcut posibilă utilizarea tehnologiei cu spectru larg neînregistrat, dar precursorul direct al Wi-Fi a fost inventat în Olanda în 1991. Scopul său inițial era să ofere suport pentru sistemul de case electronice, purta numele de WaveLAN și avea o viteză maximă de 2 Mbit/s.

Când această tehnologie a început sa fie utilizată pentru rețele au apărut numeroase probleme datorită diverselor incompatibilități dintre producătorii de produse. Standardizarea a început în 1999 cu constituirea Alianței Wi-Fi(Wi-Fi Alliance), și cu introducerea mărcii CERTIFICAT Wi-Fi, care asigura consumatorii ca produsele vor interacționa fără probleme. Wi-Fi Alliance este compania care certifică produsele după un set de teste pentru a determina interoperabilitatea. Tehnologia Wi-Fi a trecut prin mai multe faze începând din 1997. Wi-Fi este suportata de diferite extensii sub sisteme de operare precum: Microsoft Windows, Apple Mac OS X, Unix, Linux.

În plus există numeroase încercări de standardizare, care nu doar sa selecționeze componentele compatibile, ci să asigure compatibilitatea încă din timpul proiectării sau fabricării. 802.11 face parte dintr-o familie de standarde pentru comunicațiile în rețele locale, elaborate de IEEE, și din care mai fac parte standarde pentru alte feluri de rețele, inclusiv standardul 802.3, pentru Ethernet. Cum Ethernet era din ce în ce mai popular la jumătatea anilor 1990, s-au depus eforturi ca noul standard să fie compatibil cu acesta, din punctul de vedere al transmiterii pachetelor.

Standardul a fost elaborat de IEEE în anii 1990, prima versiune a lui fiind definitivată în 1997. Acea versiune nu mai este folosită de implementatori, versiunile mai noi și îmbunătățite 802.11a/b/g fiind publicate între 1999 și 2001.

Tabelul 1. Caracteristicile standardelor 802.11 folosite în Wi-Fi

Protocol	Release Date	Op. Frequency	Throughput (Typ)	Data Rate (Max)	Modulation Technique	Range (Radius Indoor) Depends, # and type of walls	Range (Radius Outdoor) Loss includes one wall
Legacy	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s		~20 Meters	~100 Meters
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	~35 Meters	~120 Meters
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	~38 Meters	~140 Meters
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	OFDM, DSSS	~38 Meters	~140 Meters
802.11n	June 2009 (est.)	2.4GHz 5 GHz	74 Mbit/s	248 Mbit/s	OFDM	~70 Meters	~250 Meters
802.11y	June 2008 (est.)	3.7 GHz	23 Mbit/s	54 Mbit/s		~50 Meters	~5000 Meters

OFDM - Orthogonal frequency-division multiplexing
DSSS - Direct-Sequence Spread Spectrum

1. IEEE 802.11a

Protocolul IEEE 802.11a folosește același nucleu ca varianta inițială a standardului, funcționează la o frecvență de banda de 5 GHz cu o rată de transfer maxim de 54 Mbit/s, care duce la rate convenabile de trecere în rețea de aproximativ de 20 Mbit/s. Faptul că funcționează la o frecvență de 5 GHz, o bandă puțin ocupată, aduce protocolului IEEE 802.11a un avantaj față de variata originală care opera în banda de 2.4 GHz. Un dezavantaj este faptul ca semnalul este mai ușor absorbit de pereți și alte obstacole.

2. IEEE 802.11b

Acest standard operează la o frecvență de bandă de 2.4 GHz, ceea ce înseamnă că semnalul său va fi în continuare afectat de interferențe provenite de la aparatele care funcționează la aceeași frecvență (cuptoare cu microunde, aparate Bluetooth, telefoane mobile), însă cu o rată de trecere mult îmbunătățita față de standard și un preț redus, el s-a impus rapid pe piața ca următorul standard.

3. IEEE 802.11g

Tot un protocol dezvoltat folosind nucleul standard, care funcționează la aceeași frecvență, dar oferă rate de transfer și de trecere mai mari, și compatibilitate cu aparatele IEEE 802.11b. Deși există aparate care integrează toate aceste protocoale, un dispozitiv care folosește exclusiv varianta b va încetini o rețea care folosește varianta g a protocolului IEEE. Din cauza faptului că funcționează la aceeași frecvență și acest protocol suferă din cauza interferențelor.

4. IEEE 802.11n

Din 2004 s-a lucrat la o nouă versiune, intitulată 802.11n și care este deja implementată de unii furnizori de echipamente. Este un protocol așteptat deoarece promite capacitatea de intrări și ieșiri multiple (MIMO).

5. IEEE 802.11y

Un standard care folosește o altă frecvență de bandă, de această dată licențiată, astfel încât nu mai există decât posibilitatea interferențelor între licențe.

Începând cu anul 2007 Wi-Fi a înregistrat un boom extraordinar, atât în domeniul afacerilor, cât și a utilizatorilor casnici, în prezent toate computerele portabile, sau telefoanele mobile nou fabricate având cel puțin o parte din facilitățile Wi-Fi [WWW18].

2.1.1. Funcția de coordonare distribuită

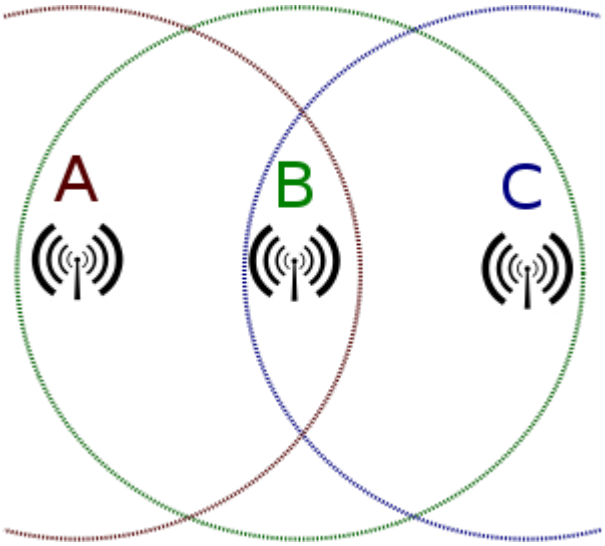

Fig. 1.Funcția de coordonare distribuită

Problema stației ascunse: A încearcă să transmită lui B în timp ce C transmite deja; A crede că nu va fi nicio coliziune.

Problema stației expuse: B vrea să-i transmită lui A în timp ce C transmite altcuiva. B crede că va avea loc coliziune la A

S-a încercat ca modelarea nivelului legătură de date a standardului IEEE 802.11 să fie cât mai similară cu standardul 802.3 (Ethernet), deja familiar implementatorilor. Realizarea controlului accesului la mediu prin tehnica CSMA/CD de la Ethernet nu este însă posibilă, deoarece caracteristicile mediului sunt foarte diferite. La Ethernet, exista întotdeauna certitudinea că, odată transmis un semnal pe mediu (cablu), acesta ajunge la toate stațiile din domeniul de coliziuni. În cazul 802.11 mediul nu mai este însă cablul, ci eterul. Domeniul de coliziuni este aici mărginit de puterea de transmisie a emițătorului radio al stației care transmite și este influențat de poziția spațială a stațiilor, ducând la probleme ca stația ascunsă și stația expusă, probleme ce afectează funcționarea CSMA/CD.

Problema stației ascunse apare când o stație A transmite unei stații B în timp ce aceasta din urmă primește mesaje de la o altă stație C, aflată în afara ariei de acoperire a lui A. A nu recepționează semnalul trimis de C, deci nu poate detecta coliziunea în caz de transmisie pe aceeași frecvență. Similar, problema stației expuse apare în exemplul de mai sus dacă B vrea să-i transmită lui A, ascultă canalul și constată că în acel moment transmite C, dar A și C nu se văd una pe cealaltă și la destinație nu ar fi nicio coliziune. Din aceste motive, CSMA/CD nu este utilizabil în contextul rețelelor fără fir.

Cum coliziunile sunt foarte greu de detectat, IEEE a recurs la o altă strategie de control al accesului la mediu, și anume CSMA cu evitarea coliziunilor (în engleză CSMA with collision avoidance, CSMA/CA). Cum canalul trebuie să fie liber și la transmițător și la destinatar, transmițătorul transmite doar când simte canalul liber. În acel moment, el trimite un cadru RTS (Request To Send) și așteaptă răspunsul o perioadă, repetând cererea dacă trece un anumit timp. Destinatarul, dacă este liber, răspunde cu un CTS (Clear To Send). După primirea CTS, transmițătorul trimite cadrul de date, după care așteaptă confirmarea receptorului. Toate stațiile altele decât cele două și care primesc un RTS sau un CTS transmis de altcineva își iau o perioadă de așteptare în care nu transmit, pentru a evita coliziunea cu cadrele transmise de celelalte stații.

2.1.2. Funcția de coordonare punctuala

În cazul funcției de coordonare punctuală, există o așa-numită stație de bază, care poate fi un punct de acces IEEE 802.11, un router cu capabilități IEEE 802.11, sau un calculator cu interfață de rețea 802.11 configurată în modul de lucru master. Această funcție de coordonare se bazează pe ideea că stația de bază este cea care controlează accesul la mediu, acordând câte o cuantă de timp fiecărui dispozitiv conectat. În acest fel, întrucât stațiile transmit doar atunci când li se permite, sunt evitate coliziunile.

Periodic, stația de bază emite un cadru-baliză (în engleză beacon frame) care conține setări privind conexiunea fizică (de exemplu, duratele de timp pentru saltul de la o frecvență la alta în cazul utilizării FHSS) și care cere stațiilor ce doresc să se conecteze să anunțe acest lucru. Stația de bază poate, de asemenea, în cazul în care poate păstra într-un buffer cadrele primite, să ceară unei stații conectate să treacă în stand-by și să o trezească atunci când aceasta a primit mai multe cadre.

2.1.3. Operarea mixtă

Cele două funcții, coordonarea punctuală și cea distribuită, nu sunt mutual exclusive, ele putând fi folosite simultan în aceeași rețea. Pentru aceasta, un cadru de confirmare (ACK) venit în urma transmiterii unui cadru de date este urmat de o perioadă de „liniște”, în care, după anumite perioade de timp, se pot trimite diferite alte tipuri de cadre (cadre baliză ale stației de bază, cadre RTS/CTS, sau cadre ce semnalează erori).

2.1.4. Topologii de rețea

O rețea Wi-Fi conține cel puțin 2 interfețe wireless lucrând conform specificațiilor 802.11. Rețeaua poate fi chiar și un laptop conectat la un alt laptop sau server (denumită într-o astfel de conjunctură și rețea ad-hoc); poate fi de asemenea constituită dintr-un număr de dispozitive wireless conectate între ele sau la un punct de acces al unei rețele.

Rețelele Wi-Fi pot fi configurate în mai multe topologii:

- topologia punct la punct;
- topologia punct la multipunct (mod bridge);
- topologia bazată pe puncte de acces (modul infrastructură);
- topologia în perechi (modul ad-hoc);
- topologia mesh.

Topologia punct la punct, constă în conectarea prin intermediul unei legături punct la punct, PTP. Printr-o legătură PTP se pot conecta direct clădiri și ca urmare elimina costurile aferente liniilor închiriate.

Topologia punct la multipunct, PMP, permite unui set de noduri să partajeze o conexiune cu un nod singular central, soluțiile PMP fiind mai economice decât PTP, deoarece în momentul în care noi noduri

dispunând de o cale de comunicație în vizibilitate directă cu nodul central sunt adăugate rețelei, nu este necesară efectuarea de modificări la stația de bază. O astfel de soluție se practică pentru conectarea unei clădiri centrale cu alte clădiri adiacente (spre exemplu într-un campus, oraș sau cartier).

Topologia bazată pe puncte de acces, AP. Într-o astfel de rețea, clienții comunică prin intermediul punctelor de acces care asigură acoperirea radio a zonei. De regulă se utilizează mai multe puncte de acces wireless amplasate astfel încât zonele acoperite să se suprapună 10÷15% pentru a permite roaming-ul.

Topologia în perechi (modul ad-hoc). Într-o astfel de rețea, dispozitivele client pot comunica direct unele cu altele, deci punctele de acces wireless nu sunt necesare. Rețeaua ad-hoc permite dispozitivelor client să comunice direct unele cu altele, fără a fi nevoie de existența unui dispozitiv de supervizare cum ar fi routerul. O caracteristică a acestei rețele este aceea că orice nod al rețelei (în particular, un computer) poate deveni membru sau poate părăsi rețeaua oricând, acest fapt putând constitui atât o calitate (reconfigurabilitate facilă a rețelei), cât și o lacună (nu se cunoaște exact numărul membrilor rețelei și identitatea acestora).

Topologia mesh poate crea rețele ce utilizează conexiuni folosind mai multe noduri intermediare pentru transmiterea pachetelor IP între nodul inițiator și cel de destinație. Abilitatea de a utiliza căi diferite de propagare, în funcție de condițiile specifice (interferență, limitări sau scăderi ale puteri semnalului, obstacole etc), deci redundanța căilor de propagare, permite ca topologia mesh să se constituie într-o rețea flexibilă, de încredere și eficientă din punct de vedere al utilizării lărgimii de bandă. În rețeaua wireless mesh pot fi adăugate / înlăturate noduri sau poate fi modificată locația acestora, acest fapt constituindu-și într-un avantaj major pe măsură ce mobilitatea populației crește, capabilități wireless sunt adăugate unor noi serii de dispozitive, iar necesitățile concrete comerciale sau domestice pot impune adaptarea sau reconfigurarea rețelei.

Alte beneficii ale topologiei wireless mesh includ costuri inițiale reduse, traficul echilibrat, mobilitatea și disponibilitatea.

În concluzie, ca urmare a analizei diferitelor soluții de configurare și având în vedere obiectivele proiectului, rețelele wireless mesh dispun de un avantaj major față de celelalte implementări din cauza faptului că rețeaua poate fi adaptată în funcție de necesități.[WWW18].

2.1.5. Avantaje, dezavantaje

Avantaje

Wi-Fi oferă posibilitatea de a dezvolta rețele fără a utiliza cablu pentru conexiunea între dispozitive, reducând astfel costul efectiv al lucrării și de asemenea, rețeaua poate fi extinsă cu costuri reduse și relativ rapid. Încăperile în care nu pot fi trase cabluri, așa cum sunt clădirile istorice, sunt un spațiu potrivit pentru rețele wireless.

Începând din 2007 adaptoare de rețea wireless sunt incluse în aproape toate laptopurile moderne. Preturile pentru chipurile necesare pentru Wi-Fi continua să scadă.

Wi-Fi este răspândita din peste 250.000 de hotspot-uri publice și în zeci de milioane de case, companii și universități. WPA (Wi-Fi Protected Access) nu este ușor de pătruns dacă sunt folosite parole puternice, iar codarea din WPA2 nu are breșe de securitate cunoscute.

	WPA	WPA2
Enterprise Mode (Business and Government)	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal Mode (SOHO/personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Fig.2.Certficate de securitate

Noile protocoale – WMM – fac WiFi-ul mai potrivit pentru aplicații cu latență sensibilă precum sunt transmisiile de date și voce, luând-se în calcul și mecanisme de diminuare a consumului de energie (WMM Powe Save) pentru a îmbunătății eficiența bateriei.

Dezavantaje

Spectrul și limitările operaționale nu sunt aceleași în întreaga lume. În mare parte din Europa sunt permise utilizare a încă 2 canale adiționale față de cele din US (1-13 vs 1-11), Japonia între 1 și 14. Un aspect care este de multe ori confundat este acela ca Wi-Fi ocupă 5 canale din banda 2,4 GHz, în loc de 3 canale în SUA: 1,6 ,11 și 4 canale în Europa: 1,5,9,13.

Puterea izotropă echivalentă radiată în Europa este limitată la 20 dBm (0.1W). Energia necesară este mai mică decât a celorlalte standarde de joasă lățime de banda, ca de exemplu Zigbee sau Bluetooth, având astfel grija de viața bateriei.

Codarea cea mai des folosita în standardele de comunicații wireless a fost Wired Equivalent Privacy – WEP, dar s-a dovedit a fi fragilă și ușor de pătruns chiar și în cazul în care este corect configurată. Wi-fi Protected Access – WEP - a fost lansat în 2003 și are ca țintă rezolvarea acestei probleme și este acum disponibil pe cele mai multe produse. Wi-fi Protected Access poate fi descrisă ca o codificare liberă. Începătorii beneficiază de o configurație de la zero a dispozitivului, ceea ce însemna că inițial, echipamentul nu are nici un standard de protecție setat, astfel fiind accesibil pentru toți utilizatorii rețelei wireless inclusiv a proprietarului, care ulterior, dacă dorește, poate să activeze un astfel de cod de protecție, restricționând astfel accesul altor utilizatori.

Multe dintre acces point-urile wireless ce folosesc standardele 802.11b, 802.11g 802.11n vin cu setări inițiale prin care se folosește același canal pentru comunicație, ceea ce conduce la congestie. Pentru a evita acest lucru, administratorul trebuie sa facă setările necesare printr-o interfață grafică.

Rețele Wi-Fi au arie de acoperire limitată. Un router Wi-Fi normal ce folosește standardele 802.11b, 802.11g, cu o antenă standard, are o arie de acoperire de circa 32 de metri în spațiu închis și 95 de metri în spațiu deschis. Aria de acoperire variază în funcție de frecvența de bandă. Pentru o frecvență mai mare (5 GHz) aria de acoperire este puțin mai mică decât pentru o frecvență mai mică (ex. 2.4 GHz). Aria de acoperire în spațiu liber poate fi îmbunătățită dacă se folosesc antene direcționale, ajungând până la câțiva kilometri dacă echipamentele sunt în linie dreaptă. De asemenea, performanțele Wi-Fi descresc proporțional pe măsura ce distanța dintre emițător și receptor crește.

Un număr excesiv de mare în aceeași arie de acoperire, în special pentru aceleași canale sau pentru canale învecinate, poate împiedica accesul și poate produce interferențe, fiind cauzate de suprapunerea canalelor din spectrul standardului 802.11b/g, dar și de scăderea raportului semnal zgomot – SNR – între acces point-uri. În plus, alte echipamente care utilizează banda de 2.4 GHz: cuptoare cu microunde, camere de securitate, bluetooth, radio amator, emițătoare video, telefoane mobile, pot cauza multe alte interferențe. Soluția generală celor care au aceste probleme sau aglomerări în rețea, este de a migra la echipamente Wi-

Fi pe 5 GHz, cum e 802.11n, deoarece banda de 5 Ghz este foarte rar folosită și dispune de mai multe canale libere [WWW18].

2.1.6. Securitatea rețelelor WI-FI

Este evident că vorbind de semnale radio, securitatea soluției fără fir este din start dezavantajată comparativ cu o soluție cablată. Problema securității a fost, până de curând, bariera principală de adoptare a rețelelor fără fir. Primele standarde de securitate s-au dovedit ineficiente și anunțurile relativ la vulnerabilitatea acestora au ținut prima pagină a presei de specialitate și au ajuns în rubrica de IT a presei generaliste. De aceea, mulți utilizatori au început să se teme de folosirea soluțiilor fără fir și pe bună dreptate.

Configurarea implicită a dispozitivelor fără fir este în general fără niciun nivel de securitate, ceea ce, pentru un utilizator fără cunoștințe avansate, este, în 90% din cazuri, configurația care va fi folosită. Acest lucru poate duce la deschiderea porților pentru accesul în rețeaua proprie al unor persoane neautorizate, care poate duce la scurgeri de date, ceea ce reprezintă un risc major.

Producătorii de echipamente fără fir se străduiesc ca instalarea și configurarea să decurgă cat mai ușor, iar toate aceste riscuri pot fi evitate în cazul folosirii soluțiilor moderne de protecție. Pentru o protecție maximă trebuie folosite chei de criptare WPA2 și o protecție suplimentară a accesului prin identificarea unică a fiecărei stații de lucru prin adresa MAC.

Rețelele wireless sunt relativ mai puțin sigure decât cele cablate, datorită accesului mai facil la rețea al persoanelor neautorizate aflate în zonele de acoperire ale punctelor de acces. Există, implicit în implementarea rețelelor wireless, diferite bariere care formează așa numita securitate de bază a rețelelor wireless, care împiedică accesul neintenționat al persoanelor străine de rețea, aflate în aria de acoperire a unui punct de acces. Pentru persoane rău intenționate, cu bună pregătire în domeniu, de tipul hackerilor, securitatea acestor rețele, ca de altfel și a altora, este discutabilă.

Barierele de securitate (securitatea de bază) care au fost prevăzute în protocoalele rețelelor Wi-Fi asigură un nivel relativ scăzut al securității acestor rețele, ceea ce le-a frânat întrucâtva dezvoltarea. În iunie 2004, s-a adoptat standardul 802.11i care îmbunătățește securitatea rețelelor wireless.

Securitatea de bază a rețelelor wireless este asigurată de următoarele funcții implementate:

- SSID (Service Set Identifiers);
- WEP (Wired Equivalent Privacy);
- Verificarea adresei MAC (Media Acces Control).

SSID este un cod care definește apartenența la un anumit punct de acces wireless. Toate dispozitivele wireless care vor să comunice într-o rețea trebuie să aibă SSID-ul propriu, setat la aceeași valoare cu valoarea SSID-ului punctului de acces pentru a se realiza conectivitatea. În mod normal, un punct de acces își transmite SSID-ul la fiecare câteva secunde. Acest mod de lucru poate fi stopat, astfel încât o persoană neautorizată să nu poată descoperi automat SSID-ul și punctul de acces. Dar, deoarece SSID-ul este inclus în beacon-ul - mici pachete de date transmise continuu de un punct de acces pentru a-și face cunoscută prezența și pentru a asigura managementul rețelei - oricărei secvențe wireless, este ușor pentru un hacker dotat cu echipament de monitorizare să-i descopere valoarea și să se lege în rețea.

WEP poate fi folosit pentru a ameliora problema transmiterii continue a SSID-ului prin criptarea traficului dintre clienții wireless și punctul de acces. Se realizează prin aceasta o autentificare printr-o cheie (shared-key authentication). Punctul de acces transmite clientului wireless o provocare pe care acesta trebuie s-o returneze criptată. Dacă punctul de acces poate decripta răspunsul clientului, are dovada că acesta posedă cheia validă și are dreptul de a intra în rețea. WEP dispune de două posibilități de criptare – cu cheie de 64 de biți sau de 128 de biți.

Desigur, WEP nu asigură o securitate prea mare. Hackerul dotat cu echipament de monitorizare poate recepționa și înregistra întâi provocarea plecată de la punctul de acces apoi răspunsul criptat al clientului și, pe baza unor procesări se poate determina cheia pe care apoi o poate folosi pentru a intra în rețea.

Verificarea adresei MAC. Se poate spori securitatea rețelei, dacă administratorul de rețea utilizează filtrarea adreselor MAC, adică punctul de acces este configurat cu adresele MAC ale clienților cărora le este permis accesul în rețea.

Din nefericire, nici această metodă nu asigură o securitate prea mare. Un hacker poate să înregistreze secvențe din trafic și, în urma unor analize, poate să extragă o adresă MAC pe care ulterior o poate folosi pentru a intra în rețea.

Îmbunătățiri ale securității rețelelor

- **802.1x:**

Este un standard de control al accesului în rețea bazat pe porturi. El asigură per utilizator și per sesiune o autentificare mutuală puternică. În funcție de metoda de autentificare utilizată, 802.1x poate asigura și criptarea. Pe baza IEEE Extensible Authorization Protocol (EAP), 802.1x permite punctului de acces și clienților din rețea să folosească în comun și să schimbe chei de criptare WEP în mod automat și continuu. Punctul de acces acționează ca un proxy server, efectuând cea mai mare parte a calculelor necesare criptării. Standardul 802.1x suportă managementul centralizat al cheilor de criptare din rețea.

- **WPA (Wi-Fi Protected Acces):**

A fost introdus ca o soluție intermediară la criptarea WEP după ce standardul IEEE 802.11g/n a fost ratificat. Când WPA este implementat, punctul de acces permite numai accesul clienților care dispun de fraza de trecere corectă. Cu toate că WPA este mai sigură decât WEP, atunci când cheile sunt memorate și la clienți, furtul unui dispozitiv-client poate permite hoțului accesul în rețea.

WPA suportă atât autentificarea cât și criptarea. Autentificarea realizată cu ajutorul cheilor prestabilite este cunoscută ca WPA Personal. Când este realizată conform standardului 802.1x, este cunoscută ca autentificare WPA Enterprise. WPA oferă ca algoritm de criptare TKIP (Temporal Key Integrity Protocol), precum și noul algoritm de integritate numit Michael. WPA face parte din standardul 802.11g/n.

- **WPA2:**

Este o certificare de produs pentru echipamentele wireless compatibile cu standardul 802.11g/n. Această certificare asigură suport și pentru proceduri de securizare suplimentare ale standardului 802.11g/n care nu sunt incluse în WPA. WPA2 ca și WPA suportă procedeele de autentificare Personal și Enterprise. WPA2 conține îmbunătățiri care facilitează roamingul rapid pentru clienții wireless aflați în mișcare. Permite o pre-autentificare la punctul de acces către care se deplasează clientul, menținând încă legătura cu punctul de acces de la care pleacă [WWW18].

2.2. Tehnologia LoRa și protocolul LoRaWAN

Termenul de LoRa (sau tehnologie LoRa) se referă la o categorie de comunicații radio caracterizate de distanță mare de transmisie (Long Range) cu un consum mic de energie (Low Power). Spre deosebire de tehnologiile de transmisie radio digitale clasice, tehnologiile LoRa au capabilitatea de a comunica date la distanțe de câțiva kilometri sau chiar zeci de kilometri având aplicabilitate extraordinară în rețele de senzori wireless (fără fir), internetul obiectelor (IoT) și crearea de rețele de dispozitive inteligente. În spatele termenului de LoRa se află de fapt o multitudine de tehnologii proprietar sau deschise, similare ca funcționalitate dar total incompatibile ca implementare – domeniul de comunicații digitale radio la distanțe mari fiind la momentul actual într-o fază de pionierat în care stabilitatea oferită de standardizare și metode de interconectare tehnologică sunt un deziderat destul de îndepărtat. Alți termeni utilizați pentru a referi

rețelele radio digitale cu raza mare de transmisie sunt: LoRaWAN (LoRa Wide Area Network), LPWAN (Low Power Wide Area Network), 6LowPAN (IPv6 Low-power Personal Area Network), LPN (Low Power Network) – unii dintre acești termeni sunt înregistrați ca mărci aparținând unor anumite companii sau consorții fiind folosiți pentru a identifica o anumită tehnologie LoRa (chiar și termenul de LoRa este marcă înregistrată a companiei Semtech).

LoRa – Tehnologie radio ce utilizează benzi de frecvență radio ISM sub-GHz pentru a transmite datele la distanțe mari cu un consum foarte mic de energie.

Este o tehnologie proprietar și este dezvoltată de compania Semtech. Specifică nivelul fizic de comunicație (modulația radio). Este implementată în circuitele integrate radio din seria SX1xxx produse de Semtech sau în circuitele RFM9x produse de HopeRF (care a cumpărat licența pentru nucleul radio LoRa). Cele două familii de circuite radio sunt compatibile deoarece implementează același nucleu electronic de comunicație radio. Există mai multe plăci de dezvoltare și module de comunicație radio bazate pe circuitele din cele două familii:

- Seeeduino LoRaWAN– placă de dezvoltare bazată pe un microcontroler ARM Cortex-M0+ ATSAMD21G18 (la fel ca și placa Arduino M0, placa este compatibilă cu mediul Arduino IDE) și un modul de comunicație radio RHF76-052 bazat pe circuitul SX1276 (compatibil LoRa).

Fig.3. Seeeduino LoRaWan

- Dragino LoRa Shield – shield Arduino bazat pe circuitul radio RFM98W (compatibil LoRa). Integrează un senzor de temperatură și indicator de baterie. Compatibil cu Arduino Uno, Leonardo, Mega.

Fig.4. Dragino LoRa Shield

- Raspberry Pi LoRa/GPS HAT – shield (hat) pentru placa Raspberry Pi 2/3. Bazat pe un modul RFM92 (compatibil LoRa). Include un receptor GPS.

Fig.5. Raspberry Pi LoRa/GPS HAT

- Adafruit Feather 32U4 / M0 RFM9x precum și shield-ul LoRa Radio Feather bazate pe module RFM9x și compatibile cu mediul Arduino IDE. Plăci de dezvoltare de mici dimensiuni, compacte și cu posibilitatea de alimentare de la un acumulator LiPo de 3.7V.

Fig.6. Adafruit Feather 32U4/M0

- Modul radio Adafruit RFM96W ce permite utilizarea modului radio de la HopeRF împreună cu diverse plăci de dezvoltare inclusiv plăcile de dezvoltare Arduino.

Fig.7 Adafruit RFM96W

LoRaWAN (LoRa Wide Area Network) – set de specificații deschise de tipul LPWAN (Low Power Wide Area Network) dezvoltate de consorțiul LoRa Alliance.

LoRa Alliance™
Wide Area Networks for IoT

Fig.8. Logo LoRa Alliance

Completează tehnologia LoRA cu nivelul MAC. Chiar dacă este un set de specificații deschise la care contribuie o serie de companii importante (CISCO, IBM, ST, Renesas, ZTE, Microchip…) se bazează în totalitate pe nivelul fizic proprietar LoRa. Totuși, există o comunitate mare de utilizatori care și-au propus construirea unei rețelei globale LoRaWAN (The Thing Network) – în prezent puteți găsi acoperire TTN la noi în țară în București și Timișoara.

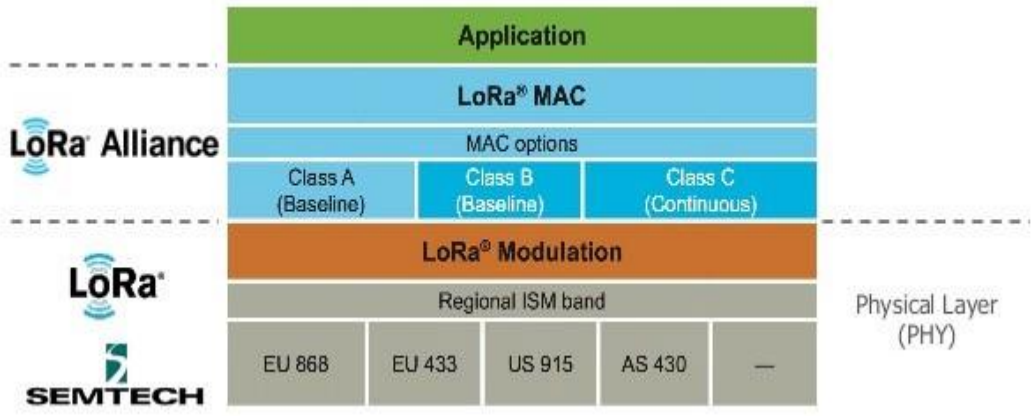

Fig.9. Tabel aplicații și benzi de frecvență

Internet of Things, Internetul Lucrurilor sau, pe scurt, IoT e un fenomen ce se află de mai mulți ani

în centrul atenției oricărui expert în materie de tehnologie, mulți dintre aceștia exagerând avantajele. Definiția termenului „IoT” diferă în funcție de specialistul care îl explică. Cel mai răspândit și cel mai scurt răspuns este că Internetul Lucrurilor este o rețea de obiecte fizice conectate la Internet.

Inițial, numeroși experți au considerat imposibil acest concept. Cu toate acestea, companii precum Procter & Gamble, Gillette, WalMart, Tesco, Canon și Coca-Cola, precum și organizațiile de stat americane (Departamentul Apărării, Serviciul Poștal) au recunoscut avantajele pe care IoT le-ar putea aduce lanțurilor lor de aprovizionare și au contribuit la stimularea dezvoltării tehnologiei.

Cine a inventat termenul „IoT”?

Lansată de pionierul în tehnologie Kevin Ashton în anul 1999, expresia „Internet of Things” desemna inițial utilizarea Internetului pentru a permite computerelor să observe lumea. Această rețea de obiecte conectate era menită să adune informații din mediul fizic care să contribuie la găsirea unei soluții pentru o problemă raportată.

Așa cum afirma Ashton într-un interviu anul trecut, IoT este o soluție care vă permite „să cunoașteți tot ce trebuie să știți despre lumea fizică. Informații precum unde se află lucrurile, unde se află clienții sau dacă lucrurile au nevoie de întreținere sau de altceva.”

2.2.1. LoRa și IoT

O definiție mai flexibilă a IoT, cea care a generat acest cuvânt-cheie al momentului, include orice gadget care se poate conecta la Internet – așa-numitele dispozitive „inteligente” (smart). De obicei, acestea sunt lucruri obișnuite, prevăzute cu cipuri care permit utilizatorilor să controleze sau să interacționeze cu ele prin intermediul unei rețele. Lista include aproape orice obiect conectat considerat, de regulă, inteligent.

Indiferent de forma acestora, dispozitivele IoT reprezintă o parte comună a vieții noastre, iar șansele ca acestea să cadă din grație în viitorul apropiat sunt mici sau chiar inexistente.

Internet of Things (IoT) este o rețea de obiecte fizice care conțin electronice încorporate în arhitectura lor pentru a comunica și a simți interacțiunile între ele sau cu mediul extern. În următorii ani, tehnologia bazată pe IoT va oferi niveluri avansate de servicii și va schimba practic modul în care oamenii își duc viața de zi cu zi. Progresele în medicină, inginerie, business, agricultură, orașe inteligente și case inteligente sunt doar câteva dintre exemplele categorice în care IoT este puternic stabilit. Cu alte cuvinte IoT este conectarea oricărui dispozitiv (de la telefoane mobile, vehicule, electrocasnice și alte elemente încorporate cu senzori și actuatori) cu Internetul, astfel încât aceste obiecte să poată schimba date între ele într-o rețea. Este interesant de menționat faptul că diferența între IoT și Internet, este absența rolului uman. Dispozitivele IoT pot crea informații despre comportamentele individuale, pot analiza și acționa (IoT este mai inteligent decât Internetul).

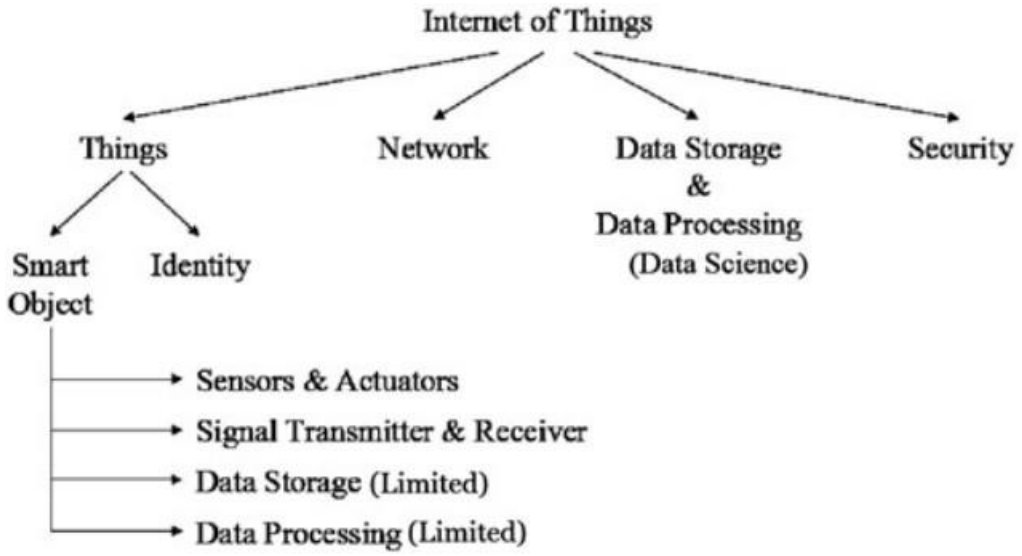

Fig.10. Arhitectura IoT

Din figura de mai sus, putem vedea că există diferite componente într-un sistem IoT. În afară de infrastructura și securitatea rețelei, o mare parte din IoT necesită stocarea și procesarea datelor pe un macroscopic (adică în sistemul de ansamblu) precum și pe un nivel microscopic (adică în fiecare Smart Object local). SO-urile în sine ar trebui să aibă unele prelucrări de date, informații și capacitate de luare a deciziilor în baza acestor informații. Pentru asta, trebuie să aibă instrumente de prelucrare a datelor încorporate, pentru a analiza datele senzorului și a face unele decizii inteligente. La nivel macroscopic și mai mult decât miliarde de lucruri vor genera date independent și ar fi transmis aceste date prin rețea la distanță, și locații de stocare diferite pentru o procesare suplimentară și toate acestea în timp real. O mulțime de date vor fi generate, stocate și prelucrate continuu.[1]

Orice Smart Object poate avea, de asemenea, o capacitate de stocare a datelor și o capacitate limitată de prelucrare a datelor. De exemplu, un ceas inteligent detectează când utilizatorul este staționar (șezând sau culcat) pentru o lungă perioadă de timp, detectează când utilizatorul doarme. Poate diferenția în mod clar atunci când utilizatorul doarme și stă. Pentru a face acest lucru, nu este necesar să se transmită date la orice server și să se efectueze o procesare la distanță. Colectează datează și face unele mici analize în sine pentru a acționa alarma. Aceste capacități de luare a deciziilor pe termen scurt sunt încorporate într-un dispozitiv inteligent. Pentru luarea de decizii pe termen lung sau pentru găsirea informațiilor, stocarea la distanță și procesare poate fi necesară.

Nu este necesar de a păstra toate datele într-un singur loc, la un moment de timp. Deci, sunt extrase porțiuni relevante mai mici ale datelor și tratate ca și când este nevoie. Datele trebuie analizate rezonabil în timp real pentru a lua decizii utile. Datele care sunt generate și gestionate de IoT sunt colectate, în esență, de către părți individuale ale IoT care formează împreună un întreg sistem. Aceste părți ale IoT sunt discutate în secțiunile următoare.

2.2.2. Rețele de senzori

Senzorii sunt o componentă cheie care ne ajută să colectăm date în timp real din mediul înconjurător. Toate aceste date pot avea diferite niveluri de complexități. Ar putea fi un senzor simplu de monitorizare a temperaturii sau poate fi sub forma unei monitorizări video in timp real. Un dispozitiv poate avea diferite tipuri de senzori care îndeplinesc mai multe sarcini în afară de detectare.

De exemplu, un telefon mobil este un dispozitiv care are mai mulți senzori precum GPS, aparat de fotografiat, senzor de câmp magnetic, sunet ș.a. Evident, senzorii și actuatorii sunt importanți pentru IoT,

dar ce sunt până la urmă? Un senzor, este un dispozitiv a cărui sarcină este de a detecta evenimente sau schimbări în mediul său imediat și de a converti aceste fenomene fizice (cum ar fi temperatura, lumina, umiditatea aerului, mișcarea, prezența substanțelor chimice și multe altele) în impulsuri electrice care apoi poate fi interpretat în mod semnificativ.

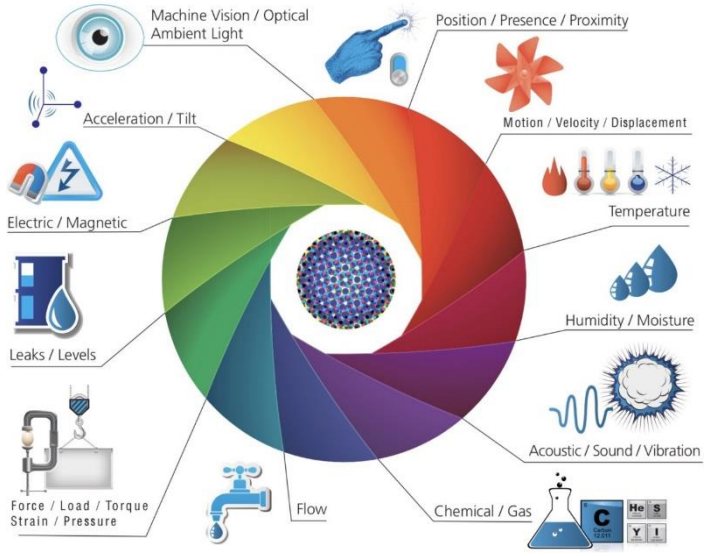

Fig. 11. Tipuri de senzori si actuatori pe care se bazează IoT

Pe de altă parte, un actuator poate fi văzut ca un instrument care funcționează invers la senzor. Interpretând impulsurile electrice transmise de la sistemul de control și transformându-le în mișcare mecanică, introduce de fapt modificări în mediul său fizic printr-o varietate de acțiuni simple, incluzând, dar fără a se limita la deschiderea și închiderea ventilelor, schimbarea poziției altor dispozitive sau unghiul, activarea lor sau emiterea de sunete sau lumină. În termini mai simpli, actuatorul este denumit „dispozitiv de mutare”. Ca senzori mai există accelerometre, senzori de temperatură, magnetometre, senzori de proximitate, giroscopuri, senzori de imagine, senzori acustici, senzori de lumină, senzori de presiune, senzori RFID cu gaz, senzori de umiditate și micro-senzori de flux. În zilele noastre avem de asemenea multe dispozitive care le putem purta, cum ar fi ceasurile inteligente și ochelarii 3D. Acesta este cel mai bun exemplu de soluție inteligentă. Ochelarii 3D ajustează luminozitatea și contrastul televizorului în funcție de ochi, iar ceasurile inteligente vă urmăresc activitățile zilnice și fitnessul, vă pot afișa informații direct pe retină, și toate acestea se fac doar avându-i pe ochi. Dar cel mai important dispozitiv care a contribuit enorm la IoT sunt telefoanele mobile. Aplicațiile mobile au contribuit enorm la revoluționarea lumii tehnologiei. Telefoanele mobile sunt deja încărcate cu aplicații și senzori care dezvăluie multe informații despre utilizatorul său. Are informații despre locația geografică, poate sesiza și urmări starea luminii, orientarea dispozitivului și multe alte informații. De asemenea, vine cu mai multe opțiuni de conectare, cum ar fi Wi-Fi, Bluetooth și celular, care îi ajută să comunice cu alte dispozitive. Astfel, datorită acestor calități implicite ale telefoanelor mobile, acesta este nucleul ecosistemului IoT. Astăzi, Smartphone-ul poate interacționa cu smartwatch-ul și formația de fitness pentru a ușura și îmbunătăți experiența utilizatorului. IoT folosește mai multe tehnologii și protocoale pentru a comunica cu dispozitivele în funcție de cerințe. Principalele tehnologii și protocoale sunt Bluetooth, wireless, NFC, RFID, protocoale radio și WiFi-Direct. Aplicațiile IoT sunt înfloritoare în toate industriile și pe piață. IoT are o multitudine de extinderi pe diverse industrii. Se întinde pe toate grupurile de utilizatori, de la cei care încearcă să reducă și să conserve energia în casa lor până la organizații mari care doresc să își îmbunătățească operațiunile de afaceri. IoT nu numai că s-a dovedit a fi util în optimizarea aplicațiilor critice în multe organizații, dar a crescut și conceptul de automatizare avansată, pe care ni l-am imaginat cu un deceniu înainte. Să înțelegem

capacitățile IoT în diferite industrii și să ne uităm cum ele revoluționează.

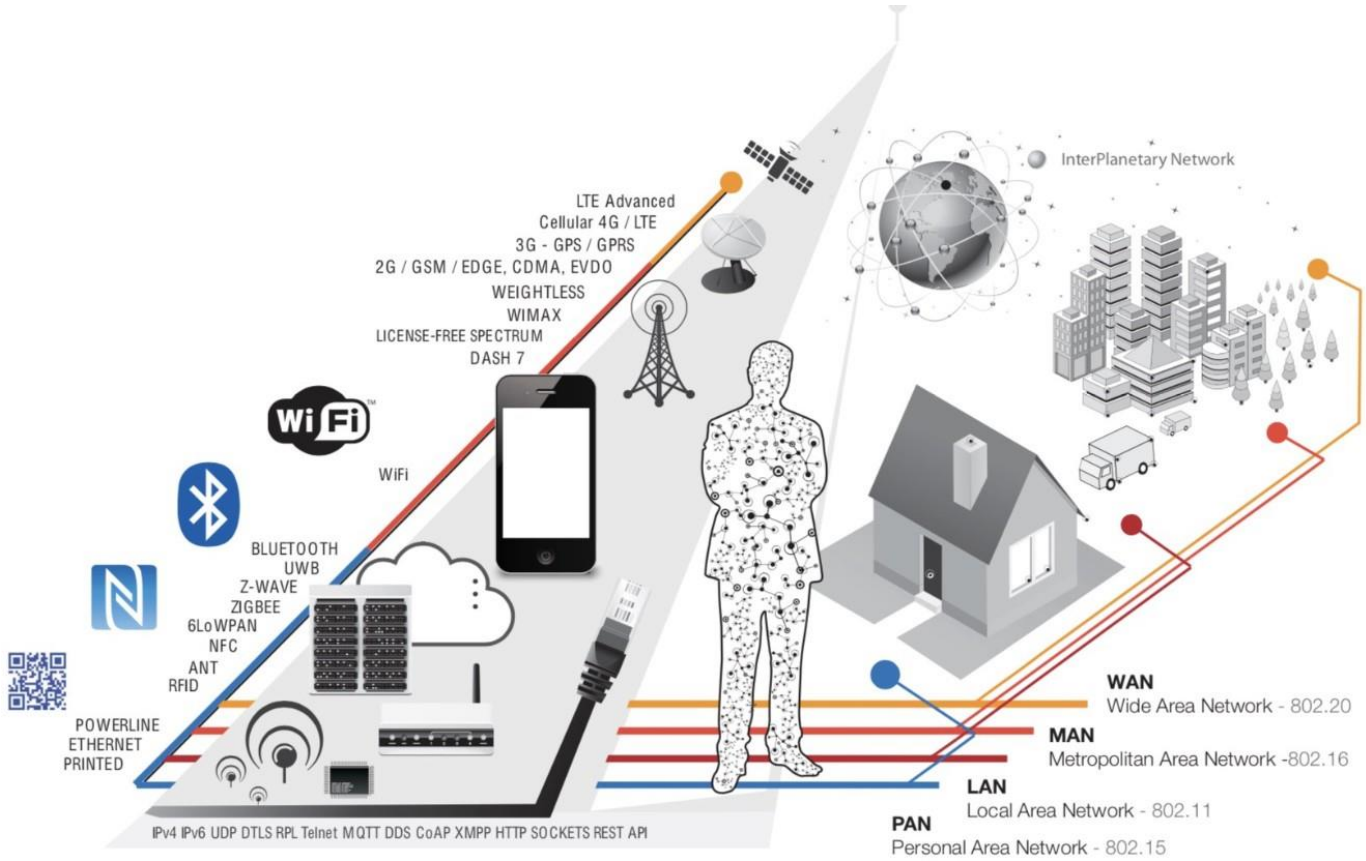

Fig.12. Tipuri de conexiuni in dispozitivele IoT

Când vine vorba de conectarea la Internet of Things, există un număr aparent copleșitor de opțiuni. Celular, satelit, WiFi, Bluetooth, RFID, NFC, WAN, LAN, LTE, 2G, 3G și altele sunt doar câteva dintre modalitățile posibile de conectare a unui senzor / dispozitiv. Opțiunea perfectă de conectare ar consuma o putere extrem de mică, ar avea o gamă uriașă și ar putea transmite cantități mari de date (lățime mare de bandă). Din păcate, această conectivitate perfectă nu există. Fiecare opțiune de conectare reprezintă o schimbare între consumul de energie electrică, intervalul și lățimea de bandă. Internet of Things este format din senzori/dispozitive conectate, deci prin definiție un sistem IoT are nevoie de un fel de conectivitate, mai ales dacă folosește cloud. Cu toate acestea, există anumite cazuri în care prelucrarea datelor sau interacțiunea cu senzorul / dispozitivul prin interfața de utilizator pot avea loc fără a fi transferate date printr-o rețea externă. Un motiv este latența, care se referă la cât timp durează un pachet de date pentru a ajunge de la punctul de pornire la punctul final. Deși latența nu contează în marea majoritate a cazurilor, pentru unele aplicații IoT, latența este esențială. Imaginați-vă că vă aflați într-o mașină cu autovehicul și deodată cineva își pierde controlul mașinii în fața voastră. Doriți să așteptați ca mașina cu autovehicul să trimită date în cloud, să fie prelucrate aceste date, apoi să aveți instrucțiuni pentru ce să faceți trimise înapoi la mașină? Nu! Aceste milisecunde ar putea însemna viață sau moarte. Un alt motiv este că trimiterea multor date poate deveni cu adevărat costisitoare. Unele aplicații IoT colectează o tonă de date, dar doar o mică parte este de fapt importantă. Algoritmii locali pot restricționa ceea ce este trimis, reducând astfel costurile.

După ce datele sunt colectate și ajung în cloud, software-ul efectuează procesarea datelor colectate. Acest proces poate fi doar verificarea temperaturii, citirea pe dispozitive precum AC sau încălzitoare. Cu toate acestea, uneori poate fi, de asemenea, foarte complex, precum identificarea obiectelor, folosind viziunea artificiala a calculatorului.

Informațiile trebuie să fie disponibile pentru utilizatorul final în așa fel încât sa fie posibilă

declanșarea de alarme pe telefoanele lor sau trimiterea notificărilor prin e-mail sau prin mesaj text. Uneori, utilizatorul poate avea nevoie de o interfață care verifică activ sistemul IOT. De exemplu, utilizatorul are o cameră instalată în casa sa. El dorește să acceseze înregistrarea video și toate fluxurile cu ajutorul unui server web. Cu toate acestea, nu este întotdeauna o comunicare unidirecțională. În funcție de aplicația IoT și de complexitatea sistemului, utilizatorul poate fi, de asemenea, capabil să efectueze o acțiune care poate crea efecte în cascadă. De exemplu, dacă un utilizator detectează modificări ale temperaturii frigiderului, cu ajutorul tehnologiei IOT, utilizatorul ar trebui să poată regla temperatura cu ajutorul telefonului mobil. Și unele acțiuni sunt efectuate automat. În loc să vă aștepte să ajustați temperatura, sistemul ar putea să o facă automat prin reguli predefinite. În loc să te sune doar pentru a te avertiza despre un intrus, sistemul IoT ar putea, de asemenea, să notifice automat echipele de securitate sau autoritățile relevante.

2.2.3. Direcții de cercetare

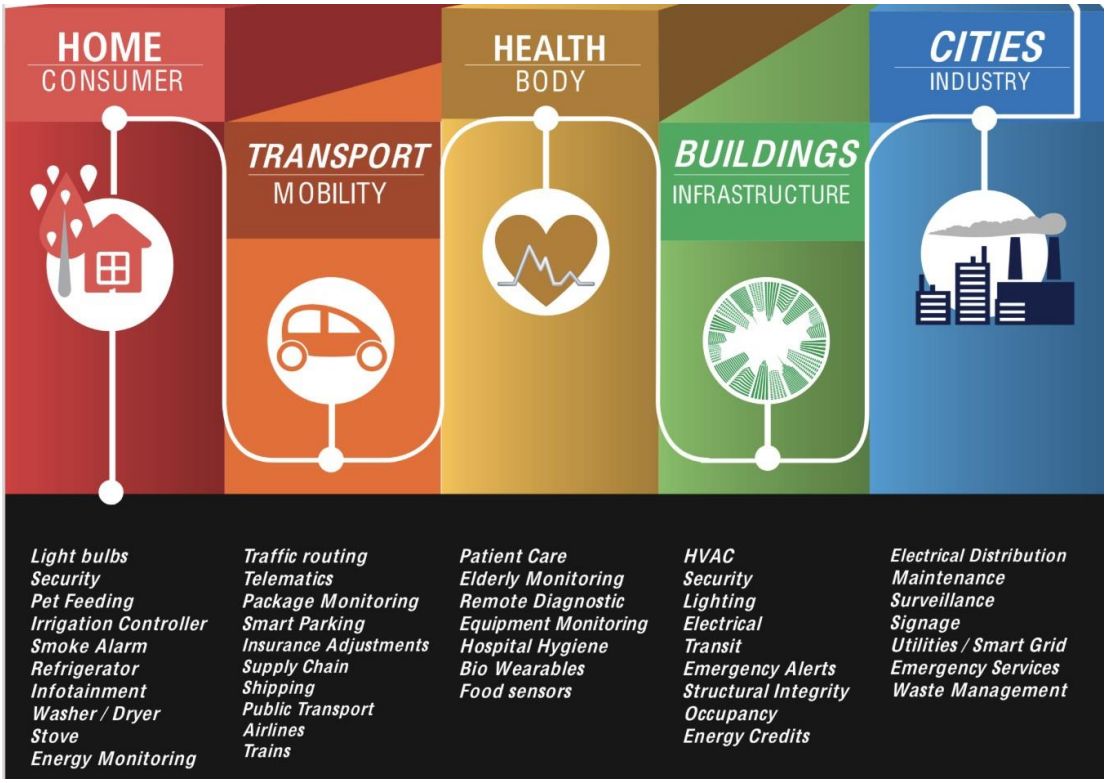

Fig.13. IoT pe diverse domenii

Domeniul medical: Ceasurile inteligente și dispozitivele de fitness au schimbat frecvența monitorizării sănătății. Oamenii își pot monitoriza propria sănătate la intervale regulate. Nu numai acest lucru, acum, dacă un pacient vine la spital prin ambulanță, la momentul în care ajunge sau la spital raportul său de sănătate este diagnosticat de medici și spitalul începe rapid tratamentul. Datele culese din mai multe aplicații de asistență medicală sunt acum colectate și folosite pentru a analiza diferite boli și pentru a găsi leacul acestora.

Societate Guvernare: Guvernele încearcă să construiască orașe inteligente folosind soluții IoT. IoT îmbunătățește sistemele și serviciile forțelor armate. Oferă o mai bună securitate peste granițe prin dispozitive ieftine și performante. IoT ajută agențiile guvernamentale să monitorizeze datele în timp real și să-și îmbunătățească serviciile precum asistența medicală, transportul, educația etc. Prin diferiți senzori, putem detecta poluarea din aer și apă prin prelevare frecventă. Acest lucru ajută la prevenirea contaminării substanțiale și a dezastrelor conexe. IoT permite operațiunile pentru a minimiza intervenția umană în analiza și monitorizarea agriculturii. Sistemele detectează automat modificări ale culturilor, solului,

mediului și altele.

Transport: IoT a schimbat sectorul transporturilor. Acum, avem autovehicule cu senzori, semafoare care pot sesiza traficul și pot comuta automat, asistență la parcare, oferindu-ne locația locului de parcare gratuit etc. De asemenea, diverși senzori din automobil indică starea actuală a vehiculului, astfel încât să nu fie probleme în timpul călătoriei.

Sectorul Privat: Și în sectorul privat Iot a avut unul dintre cele mai mari succese, casele Smart oferă posibilitatea de a automatiza majoritatea acțiunilor efectuate zilnic, de exemplu: deschiderea ușii, la apropierea dispozitivului portabil către locuință să se deschidă ușa automat, să se aprindă luminile și termostatul să acționeze cazanul, majoritatea utilităților din casă pot fi reglabile direct de pe telefon, din orice colț al lumii.

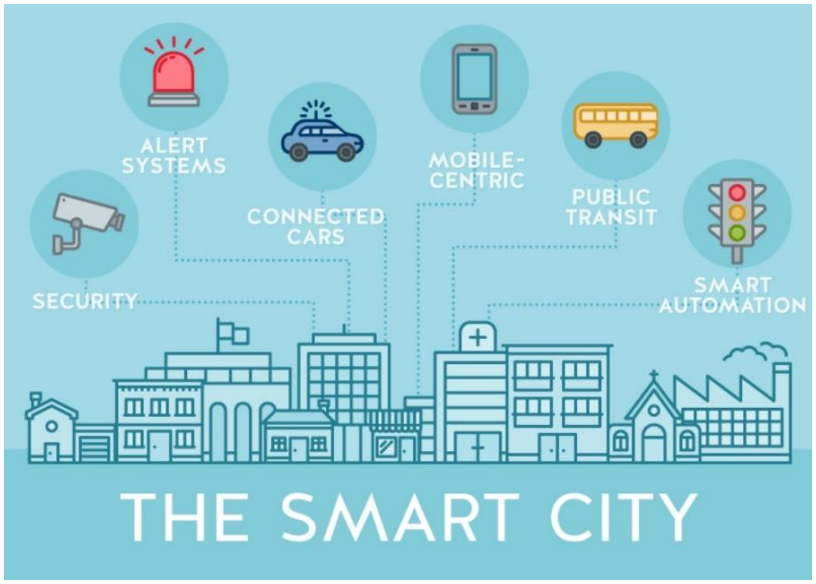

Fig.14. Posibile aplicații ale Iot în orașe

Orașe inteligente: Supravegherea inteligentă, transportul automat, sistemele mai inteligente de gestionare a energiei, distribuția apei, securitatea urbană și monitorizarea mediului, sunt exemple de aplicații pe internet pentru lucrurile Smart. IoT va rezolva problemele majore cu care se confruntă oamenii care locuiesc în orașe precum poluarea, congestionarea traficului și deficitul de aprovizionare cu energie etc. Prin instalarea de senzori și folosirea aplicațiilor web, cetățenii pot găsi spații de parcare disponibile gratuit în oraș. De asemenea, senzorii pot detecta probleme de falsificare a contorului, defecțiuni generale și orice probleme de instalare în sistemul de electricitate.

Fig.15. Dispozitive purtabile

Electronica purtabilă este electronică încorporată în diverse accesorii și îmbrăcăminte. Sunt echipate cu dispozitive miniaturizate, cum ar fi microcipuri și senzori, care posedă mai multe caracteristici ale telefoanelor mobile și laptopurilor. Aceste dispozitive electronice colectează date și urmăresc activitățile în timp real. Unele dintre aceste dispozitive sunt ochelari Google, benzi inteligente, ceasuri inteligente și monitor de îmbrăcăminte inteligent în timp real. Multe dintre echipamentele electronice purtabile dispun de tehnologie hands-free. Ceasurile inteligente au capacitatea de a apela, trimite și primi mesaje și notificări.

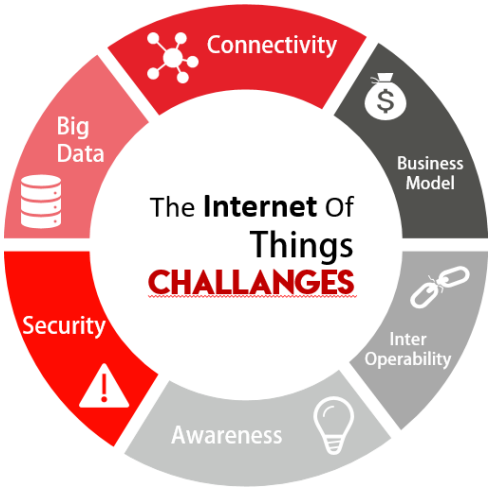

Fig.16. Provocări pentru IoT

Cercetările Gartner IoT consideră că organizațiile consideră securitatea ca fiind cea mai importantă problemă de implementare și o barieră de vârf pentru IoT. Dispozitivele conectate la internet vor fi vulnerabile la atac. Atacul a exploatat punctele slabe ale securității a mii de dispozitive IoT, permițându-le să fie deturnate. Mai mult, pe lângă dispozitivele în sine, riscurile de securitate care apar pot fi generate de platformă, de sistemul de operare, de comunicații care apar sau chiar de un sistem slab proiectat la care dispozitivul este conectat. Trebuie luate în considerare unele cerințe fundamentale de securitate în IoT, cum ar fi autorizarea, autentificarea, confidențialitatea, încrederea și securitatea datelor. Provocările sunt cum să creați și să oferiți obiective specifice de securitate pentru confidențialitate, siguranță și fiabilitate pentru părțile interesate de afaceri și să vă asigurați că dispozitivele hardware și software sunt rezistente la atacuri și capabile de securitate, prin controale hardware și software. Datele generate de lucrurile trebuie colectate, analizate, stocate, expediate și prezentate întotdeauna într-o manieră sigură în urma atacurilor software dăunătoare. În plus, Gartner prezice până în 2020, mai mult de 25% din atacurile identificate în întreprindere vor implica IoT. Obiectele inteligente, conectate, care vor popula dens Internetul Lucrurilor, vor interacționa atât cu oamenii, cât și cu mediul uman prin furnizarea, procesarea și livrarea tot felul de informații sau comenzi. Aceste lucruri conectate vor putea comunica informații despre persoane și obiecte, starea lor și împrejurimile lor și pot fi folosite de la distanță. Toată această conectivitate prezintă un risc pentru confidențialitate și scurgeri de informații.

Conștientizarea: Deși IoT oferă un potențial mare în a ajuta oamenii în multe aspecte ale vieții lor. Obține tot mai puțină atenție din partea comunității. Nu mulți consumatori știu ce înseamnă IoT. Bariera principală a dezvoltării și producției în masă a tehnologiei IoT sunt lipsa atât de conștientizare, cât și de percepție a valorii în rândul consumatorilor (conform Cercity Group Research). Lipsa de conștientizare din partea comunității apare atunci când a existat o percepție: care este importanța conectării dispozitivelor lor (ca lumini, ceasuri, frigidere și alte electrocasnice) la internet. Această percepție este într-adevăr principalul obstacol în calea dezvoltării atriei IoT. Valoarea percepută din partea clienților este urmată, de asemenea, cu probleme de cost, securitate și confidențialitate. Lipsa de conștientizare rezultă și din sectorul industriei, unde nu multe întreprinderi știu despre această tehnologie sau chiar dacă știu, majoritatea întreprinderilor

se confruntă încă cu probleme care vor conduce această inițiativă. Liderii, în acest caz, ar trebui să înceapă să exploreze cazurile de utilizare legate de IoT care sunt adecvate pentru a fi aplicate în organizațiile lor în direcția digitalizării și să se concentreze pe obiectivele specifice ale afacerii, având cea mai bună foaie de parcurs pentru a crea valoare semnificativă, mai degrabă decât să vorbească despre IoT în general.

Criptarea datelor: Aplicațiile IoT colectează tone de date. Preluarea și prelucrarea datelor este parte integrantă a întregului mediu IoT. Majoritatea acestor date sunt personale și trebuie protejate prin criptare. Criptarea este utilizată pe scară largă pe internet pentru a proteja informațiile utilizatorilor care sunt trimise între un browser și un server, inclusiv parole, informații de plată și alte informații personale care ar trebui considerate private. Organizațiile și persoanele fizice folosesc criptarea pentru a proteja datele sensibile stocate pe computere, servere și dispozitive mobile precum telefoane sau tablete.

Provocări de conectivitate: Miliarde de dispozitive de pe un server centralizat este una dintre cele mai mari provocări pentru IoT în viitor este de a conecta un număr mare de dispozitive și cantități masive de date pe care toate aceste dispozitive le vor produce. Va trebui să aflați o modalitate de a stoca, urmări, analiza și sensul sumelor vaste de date care vor fi generate. În prezent, ne bazăm pe modelul centralizat, server / client pentru a autoriza, autentifica și conecta mai multe noduri prezente în rețea. Acest model este suficient pentru numărul de dispozitive IoT care sunt în prezent parte din ecosistem. Cu toate acestea, în viitor, când sute de miliarde de dispozitive se vor alătura rețelei, va fi dificil să gestionați toate datele. Mai mult, capacitatea serverelor cloud actuale este atât de mică încât pot fi supraîncărcate dacă trebuie să gestioneze cantități mari de informație.

Scalabilitate: IoT înseamnă milioane de dispozitive conectate. Aceasta solicită două tendințe majore precum integrarea datelor și „datele mari”. Înseamnă că toate tipurile de date vor fi generate din acest sistem, și acestea trebuie să fie combinate. Amestecul seturilor de date mici cu seturi de date mari și seturile mari de date cu seturi de date și mai mari necesită abordări diferite. În plus, pe măsură ce vor fi făcute noi inovații, vor apărea noi tipuri de dispozitive. IoT va trebui să țină pasul cu acestea de asemenea. Scara dispozitivelor va crește și va impune o greutate mare asupra aspectului de conectivitate. Sistemul inițial ar trebui să fie capabil să gestioneze modificările din structura sa internă. Ar trebui să fie posibilități de schimbare în viitor, fără modificări semnificative la structura originală.

Energie și mediu: Majoritatea dispozitivelor pe care noi le utilizăm în prezent funcționează pe baterie și au un termen de valabilitate foarte limitat. Pe măsură ce IoT câștigă popularitate, numărul de dispozitive și dimensiunea rețelei va crește destul de rapid. Pe baza disponibilității de energie, ar fi imposibil să alimentăm aceste miliarde de dispozitive minuscule, alături de rețeaua completă din întreaga rețea glob. În cele din urmă, va trebui să trecem la surse mai neconvenționale de energie pentru utilizare prelungită. Dacă viitoarele dispozitive au o durată de valabilitate foarte scurtă precum cea de acum, s-ar genera o cantitate uriașă de e-deșeuri. Atunci ar fi imposibil ca mediul să păstreze în echilibrul și natura va fi în pericol. Astfel, pentru dezvoltarea viitoare a IoT, dispozitivele individuale, precum și sistemul total ar trebui să fie ecologic. Dezvoltarea în IoT va solicita cercetare în domeniul resurselor de energie neconvenționale sau regenerabile; cercetarea pentru realizarea dispozitivelor care vor avea o durată de valabilitate îndelungată și în domeniul reutilizării și reciclării resurselor.

Pentru construirea prototipului s-au analizat și s-au identificat următoarele componente hardware:

2.3. Microcontroler, senzori și placa de dezvoltare

Arduino Uno R3 este o placă de dezvoltare bazată pe microcontrolerul ATmega328. Are 14 pini de intrare/ieșire (dintre care 6 pot fi folosiți ca ieșiri PWM), 6 intrări analog, un oscilator de 16MHz, o

conexiune USB, mufă de alimentare, și un buton de resetare.

Caracteristici tehnice:

- Microcontroler ATmega328
- Tensiune de operare: 5V
- Tensiune de alimentare recomandată: 7-12V
- Limită de tensiune: 6-20V
- Pini intrare/ieșire digitali: 14 (dintre care 6 pot oferi ieșire PWM)
- Pini analogici de intrare: 6
- Memorie Flash 32 KB
- SRAM 2 KB
- EEPROM 1 KB
- Frecvență de lucru: 16 MHz

Fig. 17. Arduino UNO R3 [WWW4]

2.3. Senzoristică

2.3.1. Modul senzor tensiune ZMPT101B

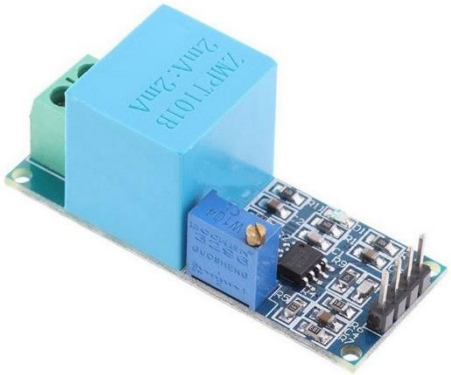

Fig. 18. Senzor tensiune ZMPT101B

Senzorul este un dispozitiv tehnic care reacționează calitativ sau cantitativ prin proprii mărimi măsurabile, la anumite proprietăți fizice sau chimice ale mediului din preajma lui. Ca parte componentă a unui aparat sau sistem tehnic detector poate măsura/înregistra de exemplu presiunea, umiditatea, câmpul magnetic, accelerația, forța, intensitatea sonoră, radiații ș.a.

Senzorul este un dispozitiv care măsoară o mărime fizică (masă, presiune, temperatură, umiditate etc.) și o transformă într-un semnal care poate fi citit de către un observator printr-un instrument sau poate fi prelucrat.

Acest modul este ideal pentru măsurarea unei tensiuni de curent alternativ. La conectarea la bornele cu șurub senzorul va încerca intrarea și ieșirea unei tensiuni analogice, în domeniul 0-5V. Acest lucru facilitează utilizarea în aplicațiile de monitorizare a energiei și verificarea consumabilelor.

Caracteristici tehnice:

- Dimensiune: 50mm x 20mm x 21.5mm
- Tensiune: 5V-30V
- Detectare până la 250V AC
- Calibrare prin potențiometru
- Chipset: ZMPT101B
- Conectori: Terminale cu șuruburi [WWW2].

2.3.2. Senzor non-invaziv de curent cu efect Hall HSTS016L

Acest senzor este utilizat pentru măsurarea curentului alternativ, reprezentând o soluție ideală pentru acest proiect.

Senzorul poate fi conectat direct pe faza pe care se dorește măsurarea, fără a fi nevoie să se facă vreo modificare.

Aplicații:

- Măsurarea curentului
- Monitorizarea curentului

Specificații:

- Curent intrare: 0 ~ 150A AC
- Mod de ieșire: 2.5 ~ 0.625V
- Acuratețe: 1%
- Non-liniaritate: < 0.1%
- Rata de conversie: 100A: 0.05A
- Temperatura de lucru: -10 ℃ ~ + 70 ℃
- Temperatură de depozitare: -40 ~ + 85 ℃
- Rezistența dielectrică: 2.5 kV AC / 1min 15mA
- Lungimea cablului: 0.5m
- Masă: 70g
- Timp de răspuns: 〈3μ s [WWW3]

Fig. 19. Senzor de curent HSTS016L

2.3.3. Senzor de curent alternativ non-invaziv 100A SCT-013

Descriere:

Acest senzor este utilizat pentru măsurarea curentului alternativ, fiind este util pentru măsurarea consumului de energie electrică.

Senzorul poate fi conectat direct pe firul de curent pentru care se dorește măsurarea, fără a fi nevoie să se facă vreo modificare sau taiere a acestuia.

Aplicații:

- Măsurarea curentului
- Monitorizarea si protecția motorului

Specificații:

- Curent intrare: 0 ~ 100A AC;
- Mod de ieșire: 0 ~ 50mA;
- Non-liniaritate: ± 3%;
- Rata de conversie: 100A: 0.05A;
- Grad rezistenta: Grad B;
- Temperatura de lucru: -25 ℃ ~ + 70 ℃;
- Rezistența dielectrică: 1000V AC / 1min 5mA;
- Lungimea cablului: 1m;
- Dimensiune senzor: 13mm x 13mm [WWW15].

Fig. 20. Senzor de curent alternativ non-invaziv 100A SCT-013

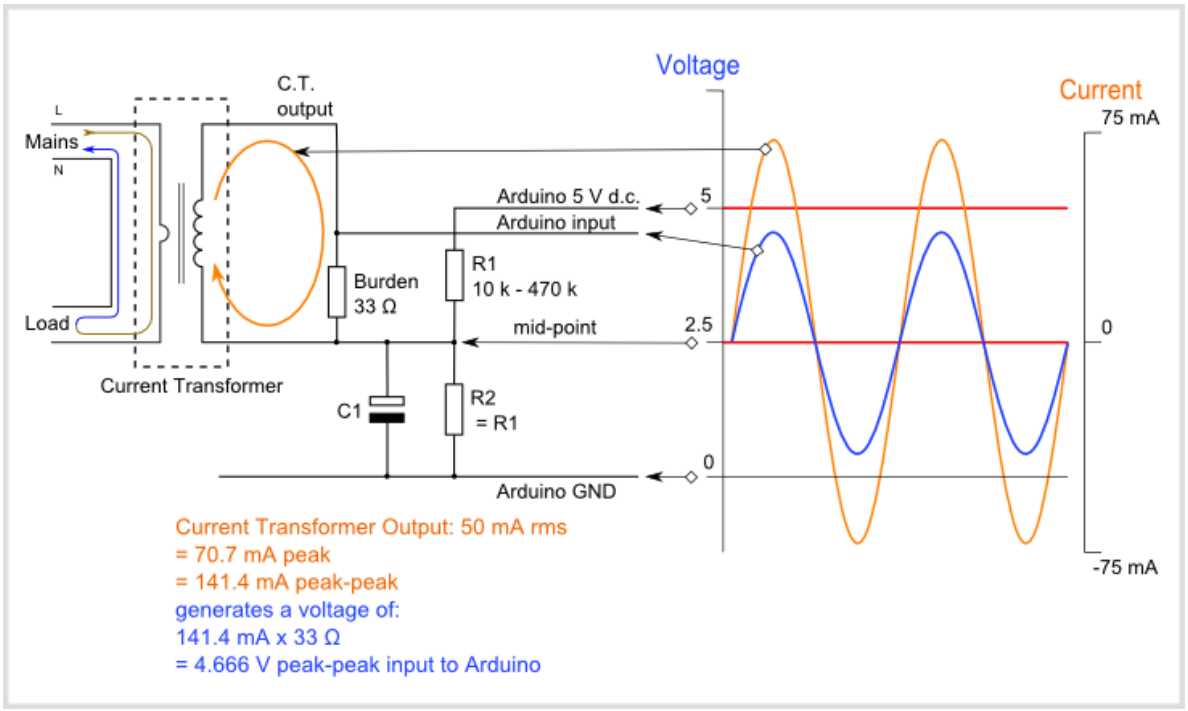

Fig. 21. Model de conectare a senzorului la Arduino [WWW16].

2.3.4. Senzor de curent alternativ non-invaziv 30A SCT-013-030

Descriere:

Acest senzor este utilizat pentru măsurarea curentului alternativ, fiind este util pentru măsurarea consumului de energie electrică.

Senzorul poate fi conectat direct pe firul de curent pentru care se dorește măsurarea, fără a fi nevoie să se facă vreo modificare sau taiere a acestuia.

Aplicații:

- Măsurarea curentului;
- Monitorizarea si protecția motorului;

Specificații:

- Curent maxim: 30A AC;
- Tensiunea de ieșire: 1V/30A;
- Rezoluție: ±1%;
- Model: SCT 013-30A;

- Producător: YHDC;
- Temperatura de lucru: -25℃～+70℃;
- Tensiunea de lucru : 660V;
- Frecvența: 50Hz-1KHz [WWW28].

Fig. 22. Senzor de curent alternativ non-invaziv 30A SCT-013-030

2.3.5. Modulul de wireless

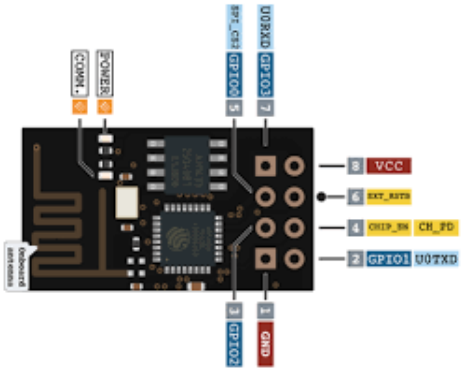

Fig.23. Modul wireless ESP8266

Acest modul funcționează la o tensiune de 3.3V și este indicat folosirea lui cu această tensiune deși izolația componentelor rezistă până la 5V.

În timpul funcționarii acest modul poate să necesite un curent de până la 380 mA ceea ce ne obligă să adăugam o sursă externă de 3.3V deoarece pinul de 3.3V de la Arduino are o limitare la 50mA MAX.

Pinii RX și TX ai acestui modul sunt folosiți tot la tensiunea de 3.3V iar pini de Arduino sunt la 5V ceea ce ne obliga să folosim fie un divizor de tensiune fie un convertor de nivel logic cu 4 canale .

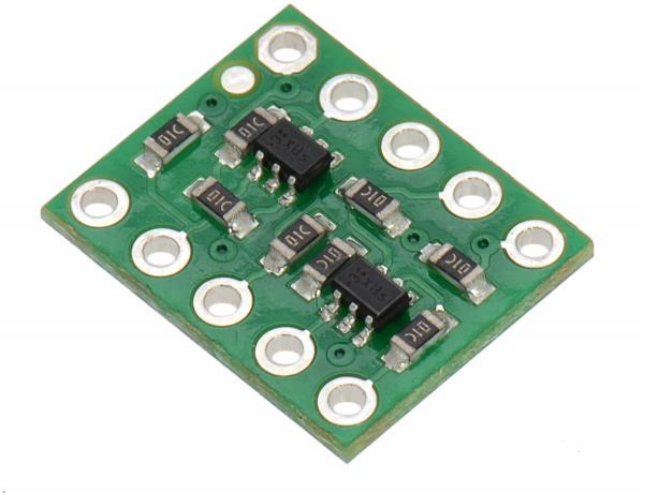

Fig.24. Convertor nivel logic 4 canale

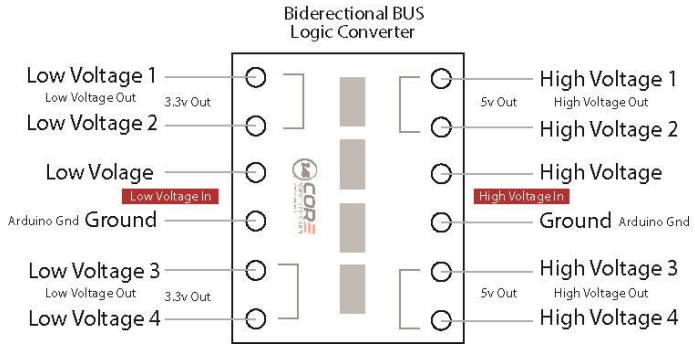

Fig.25. Schema convertorului nivel logic 4 canale

Fig.26 Sursa de alimentare

2.4. Hardware pentru comunicații

2.4.1. Dragino LoRa Shield 868Mhz

Modul LoRa de mai sus se conectează direct pe plăcuța Arduino și are rolul de a transforma datele primite de la microcontroler în unde radio.

Shield-ul Dragino LoRa este un transciever de mare distanta pentru Arduino care funcționează cu o librărie open source.

Acest shield permite utilizatorului sa transmită seturi de date la distante foarte mari.

Shieldul este bazat pe modulul RFM98W și se adresează aplicațiilor profesionale care implică rețele de senzori, cum ar fi sisteme de irigare, orașe inteligente, detectare de smartphonuri, măsurători

inteligente, etc.

Specificații:

- Compatibil cu platforme Arduino de 3.3v și 5v
- Frecventa de operare: 868 MHz / 433 MHz
- Consum redus de energie
- Antena externa prin conectorul I-Pex
- Maxim 168 dB
- +20dBm - 100mW ieșire constantă
- +14dBm eficienta
- Bit Rate programabil pana la 300 kbps
- Sensibilitate pana la -148dBm[WWW4]

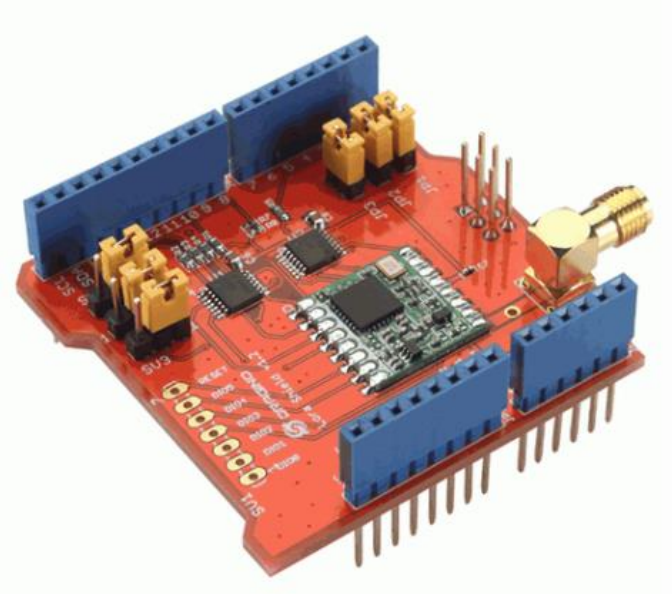

Fig. 4.6. Shield Dragino LoRa de 868 Mhz

2.4.2. Dragino LG01-N Single Channel LoRa IoT Gateway

Fig. 4.7. Gateway Dragino LG01-N

Gateway-ul are rolul de a capta undele transmise de modulul LoRa și de a le transforma în date care vor fi introduse în IoT de unde cu ajutorul unei interfețe vom putea vizualiza datele colectate.

Specificații:

- Partea Linux:
- Procesor: 400MHz, 24K MIPS
- Bliț: 16 MB; RAM: 64 MB
- Celular 4G LTE
- Modulul Quectel EC25 LTE
- Slot Micro SIM
- Antena 4G internă + Antena externă 4G.
- Până la 100 Mbps downlink și 50 Mbps rate de date în sus
- Acoperire globală LTE, UMTS / HSPA + și GSM / GPRS / EDGE
- Tehnologia MIMO satisface cerințele privind rata de date și fiabilitatea legăturilor în sistemele de comunicații fără fir modem

Interfețe:

- 10M / 100M Porturi RJ45 x 2
- WiFi: 802.11 b / g / n
- LoRa Wireless
- Putere de intrare: 12V DC
- Conector gazdă USB 2.0 x 1
- Interfață internă gazdă USB 2.0 x 1
- 1 x Interfață LoRa [WWW5]

3. Concluzii

În această etapă a proiectului s-au stabilit mărimile de instrumentație care să fie monitorizate cu ajutorul dispozitivului. În urma stabilirii cerințelor s-au analizat tehnologiile disponibile atât din punct de vedere hardware cât și din punct de vedere comunicații date.

De asemenea, după stabilirea tehnologiilor s-a efectuat o analiză și o descriere ale acestora în vederea trecerii în următoarea etapă a proiectului, și anume construirea prototipului proiectului.

În vedea îndeplinirii indicatorilor din cadrul proiectului, referitoare la publicarea a cel puțin două lucrări în reviste cotate in baza de date Weg of Science cu menționarea afilierii la AOȘR; a fost publicată și indexată o lucrare în revista MDPI Symmetry, factor de impact 2.94, cu identificator doi.org/10.3390/SYM14071351.