Universitatea Politehnica Bucuresti

Facultatea de Electronica, Telecomunicatii si Tehnologia Informatiei

RETELE DE CALCULATOARE SI INTERNET

Specificatii de nivel retea si transport in dezvoltarea aplicatiilor de tip M2M

- Dirijarea (rutarea) in IoT -

Conducător ştiinţific,
Conf. Dr. Ing. Ştefan Stăncescu

Masterand,
Camelia CHELARU
Master IISC, An II

Bucuresti 2016

Specificatii de nivel retea in dezvoltarea aplicatiilor de tip M2M -

Dirijarea (rutarea) in IoT -

Cuprins:

1. *Conceptele IoT si M2M* **3**

1.1 Notiuni si cuvinte cheie 3

1.2 Sectoarele de utilitate - M2M 5

2. *Specificatii IPv6 in M2M* **5**

2.1 Constrangeri de energie - 6LoWPAN 6

2.1.1 Concept 6

2.1.2 Compresia header-ului in 6LoWPAN - IPHC 9

2.1.3 6LoWPAN vs. ZigBee 9

2.2 Constrageri de arhitectura si scalabilitate - RPL (Routing Protocol for Low-Power and Lossy Networks) 10

2.2.1 Topologie 11

2.2.2 Formatul mesajului si transportul 12

3. *Optimizarea retelei pentru M2M* **13**

3.1 Adresare si identificare 14

3.2 Controlul congestiei 15

4. *Concluzii* **17**

Bibliografie **18**

1. Conceptele IoT si M2M

1.1 Notiuni si cuvinte cheie

IoT, în engleză Internet of Things, este Internetul Lucrurilor sau Internetul a Orice conform traducerii Wikipedia. Internetul lucrurilor este practic o rețea de obiecte: dispozitive, vehicule, clădiri și alte obiecte in care sunt încorporate componente electronice, software, senzori, și care au conectivitate la rețea, ce permite acestor obiecte colectarea și schimbul de date.

Internetul lucrurilor permite obiectelor să fie detectate și comandate de la distanță de-a lungul întregii infrastructuri a rețelei existente. Astfel se creeaza oportunități pentru integrarea mai directă a lumii fizice în sistemele bazate pe calculatoare, avand ca rezultat o eficiență sporita, mai multa acuratețe și beneficii economice. Atunci cand IoT este completat cu senzori si elemente de acționare, tehnologia devine instanță a unei clase mult mai generale a sistemelor cibernetice fizice, care cuprinde, de asemenea, tehnologii, cum ar fi rețelele electrice inteligente, case inteligente , transport inteligent și chiar orașe inteligente. [1]

Fiecare lucru este identificabil în mod unic printr-un sistem electronic incapsulat si este in acelasi timp capabil să coopereze cu infrastructura retelei de internet existenta. Experții estimează că IoT va fi alcatuit din aproape 50 de miliarde de obiecte până în 2020. [2]

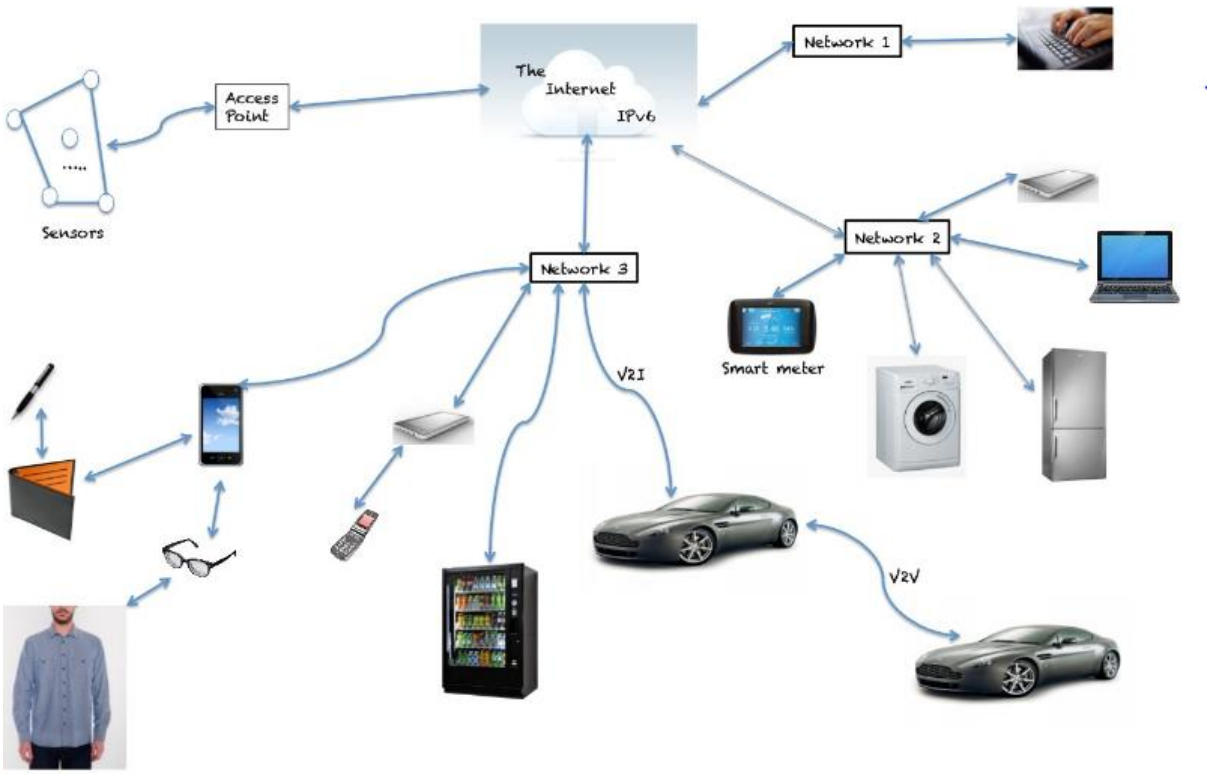

Fig. 1 Raspandirea IoT

Internet of Things oferă conectivitate si interactiuni inteligente avansate intre dispozitive, sisteme si servicii, adica o comunicare masina catre masina sau in engleza machine-to-machine (M2M). Internetul lucrurilor nu poate exista fara aceasta comunicare M2M iar comunicarea M2M poate exista decat in contextul IoT. In acest context “masinile” sunt suficient de inteligente pentru a comunica, infrastructura a fost adaptata si un nou set de standarde a fost conceput pentru a facilita aceasta comunicare - pe scurt intre M2M si IoT exista o interdependenta. [3]

M2M se refera la comunicarea directa dintre dispozitive folosind orice canale, inclusiv cu fir sau wireless. Aceasta comunicare poate de exemplu include aparatura industriala, precum programarea unui senzor care sa transmita datele pe care le inregistreaza (temperatura, presiune etc) catre o aplicatie software care le poate folosi pentru a ajusta un proces industrial. [4]

Multe aplicatii M2M au nevoie de a furniza si procesa informatii in timp real, iar pentru a reduce costurile si impactul asupra mediului se folosesc transmisii radio de mică putere pentru a se conecta la Internet.

Pentru raze mici, zone locale exista o multime de tehnologii wireless printre care: RFID, NFC, Wi-Fi, BlueTooth, XBee, zigBee, Z-Wave [3]. Pentru conectivitate de raza mare si zone extinse se pot folosi linkurile existent in retele mobile de GSM/GPRS/3G/LTE si conexiunile satelitare. (+ SIGFOX NeulNet)

IOT are nevoie de o capacitate de procesare si stocare scalabila si masiva, ce in mare masura va fi mentinuta in cloud, exceptie fac cazurile sensibile de securitate. Date si informatiile analizare din IoT vor fi disponibile utilizatorilor in mod accesibil si prin interfete navigabile.

Retelele de telefonie au evoluat de la 1G analogice in 1980 proiectate in special pentru voce la retele moderne, digitale 4G ce suporta voce de calitate ridicate, mesagerie si servicii de date. Zona de core este partea centrala a unei retele de telecomunicatii, avand functionalitatea de a ruta apelurile si datele intr-o retea. In 4G s-a produs o migrare la o solutie flexibila unde tot este bazat pe rutarea pachetelor pentru voce si date. [3]

1.2 Sectoarele de utilitate - M2M

Fig. 2 - Sectoarele de utilitate - M2M

2. IPv6 in M2M

Protocoalele dezvoltate pentru Internetul actual nu fac fata constrangerilor impuse de M2M. Limitarile consumului de energie nu au fost luate in calcul. Auto-configurarea pentru oferirea unor servicii standard va fi necesara, mai ales pentru ca dispozitivele conectate nu vor dispune neaparat de o tastatura si nu vor permite mereu configurarea manuala sau de la distanta.

Pentru a suporta M2M si WSN (retelele de senzori wireless) evolutia Internetului trebuie sa acopere o redefinire drastica a header-elor, formatelor, protocoalelor, algoritmilor de routare si a design-ului aplicatiilor cu un rol revizuit al adreselor. Pe de alta parte, interoperabilitatea cu echipamentele si aplicatiile curente este necesara, efortul de a integra IP-ul devenind altfel inutil. [7]

Internetul trece momentan printr-o perioada de evolutie a protocoalelor sale: formatul pachetelor este schimbat pentru a include 128 biti (IPv6) fata de cei 32 de biti folositi initial (IPv4). Protocolul IPv6 este o simplificare a IPv4 care pastreaza acelasi principiu. Fragmentarea a fost eliminata din header-ul pachetului, care este acum vazut ca o extensie. Asta conduce la o structura mai simpla a pachetului cu campuri mai stabile si mai predictibile. Astfel, desi lungimea adresei este de patru ori mai mare, marimea header-ului este doar de doua ori mai mare decat in cazul IPv4, asa cum este ilustrat in Figura. 3, de mai jos.

Singurul nou camp introdus de IPv6 este Flow Label (eticheta fluxului). In primele zile ale conceperii IPv6, flow label avea rolul de a usura identificarea fluxului in interiorul retelei, pentru ca numerele porturilor de Layer 4 nu erau atat de usor

accesibile in IPv4 din cauza utilizarii extensiilor. Intre timp, odata cu definirea protocolului MPLS (multiprotocol label switching) conceptul de fluxuri a fost redefinit, utilizarea acestor etichete de flux devenind mai putin importanta.

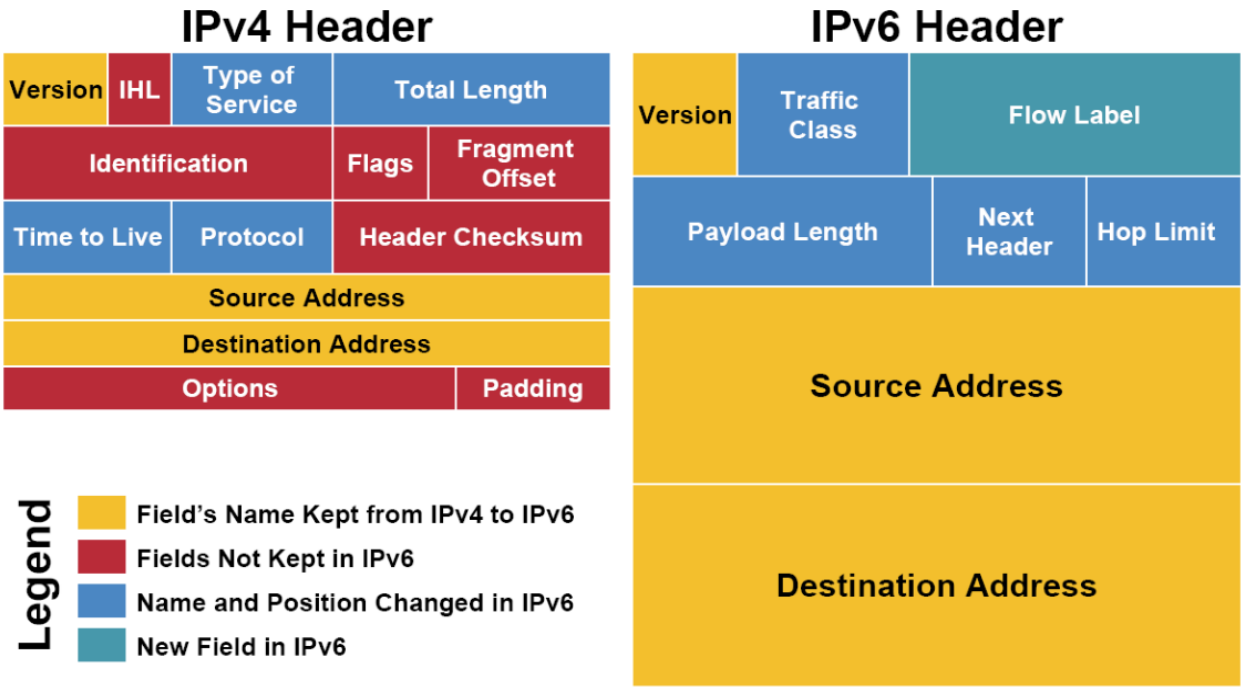

Fig. 3 - Header IPv4 vs IPv6

2.1. Constrangeri de energie – 6LoWPAN

2.1.1 Concept

Grupul 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) are ca obiectiv adaptarea protocoalelor IPv6 care pot fi suportate de retelele LoWPAN. Principalul lor tel este asigurarea compatibilitatii dintre Internet si retelele de senzori WSN pentru a adapta IPv6 si protocoalele associate la specificatiile retelei LoWPAN. [8]

Protocolul 6LoWPAN este implementat in nodurile senzor si in unul sau mai multe routere de frontiera LBR (LoWPAN Border Router) conectate la Internet. Dispozitivul LBR contine functii de routare si totodata poate compresa si decompresa pachete. Exista anumite constrangeri care cer adaptarea IPv6 la mediul LoWPAN:

- Marimea cadrului pentru Layer 2 poate fi limitata in comparatie cu specificatiile Ipv6, cu un minim obligatoriu al MTU (maximum transmission unit – cea mai mare PDU care poate fi transmisa mai departe in retea la nivelul unui anumit layer) de 1280 octeti. Va fi nevoie de fragmentare pentru a pastra lungimea cadrului specificata ce cerintele IPv6.

- Resursele de energie pot fi foarte limitate in unele noduri. De exemplu anumite dispozitive de masura pot functiona multi ani (pana la 15) folosind aceeasi baterie. Traficul multicast si schimburile ce nu sunt necesare trebuie evitate pentru a salva energie.
- Mesajele pentru descoperirea vecinilor nu trebuie sa fie fragmentate. Daca anumite fragmente sunt pierdute, protocolul devine ineficient.
- Acoperirea undelor radio poate fi redusa iar pachetul IPv6 va trebui retransmis din nod in nod pentru a atinge destinatia sau routerul de frontiera.
- Vecinii nu sunt atat de bine definiti ca in retelele clasice sau WiFi iar variatiile acoperirii radio pot provoca schimbari in lista vecinilor.

O retea 6LoWPAN poate fi organizata in trei topologii:

- Topologia Stea: toate nodurile senzor pot comunica cu routerul de frontiera si viceversa
- Topologia Mesh: nodurile sunt organizate la nivel de Layer 2 pentru a transmite cadrele catre destinatie. Nu exista algoritmi definiti de reteaua 6LoWPAN, pur si simplu facandu-se broadcast si retransmitere pas cu pas (hop-by-hop bridging).
- Topologia routata: nodurile functioneaza ca routere si transmit pachetele catre destinatie. Un protocol de routare trebuie sa ruleze pe cateva noduri pentru a construi un sistem de retransmitere a informatiei. Nodurile care se comporta ca un router in interiorul retelei LoWPAN si nu sunt conectate direct la Internet se numesc routere LoWPAN (LR). 6LoWPAN se refera la aceasta tehnologie cu denumirea de “ruta peste” (RO sau route-over). Cel mai bun candidat este protocolul RPL.

6LoWPAN nu poate fi relationat cu o anumita forma de tehnologie. Cu toate acestea implementarile actuale se bazeaza in principal pe standardul IEE 802.15.4. Patru tipuri de cadre sunt definite in aceasta retea: semnal (beacon), date, confirmare (acknowledgment) si control, asa cum se poate observa in figura de mai jos. Fiecare incepe cu un preambul de 32 de biti si un delimitator al inceputului de frame (start frame delimiter) care sa sincronizeze receptorii. Acestea sunt urmate de lungime, codata pe 7 biti permitand pana la 127 octeti de date. Prin urmare un camp de control al cadrului (frame-control) ofera informatii despre tipul cadrului, prezenta si marimea adresei sursa si destinatie (16 sau 64 biti) si un identificator al retelei personale (PANid). O secventa numerica este folosita pentru a identifica si confirma cadrele. Confirmarile nu sunt folosite cand cadrele contin un camp de adresa alcatuit din PANid si adresele sursei si destinatiei. Doar cadrul de confirmare este gol, celelalte continand date. Toate cele patru tipuri de cadru se incheie cu un CRC (control redundant ciclic). [8]

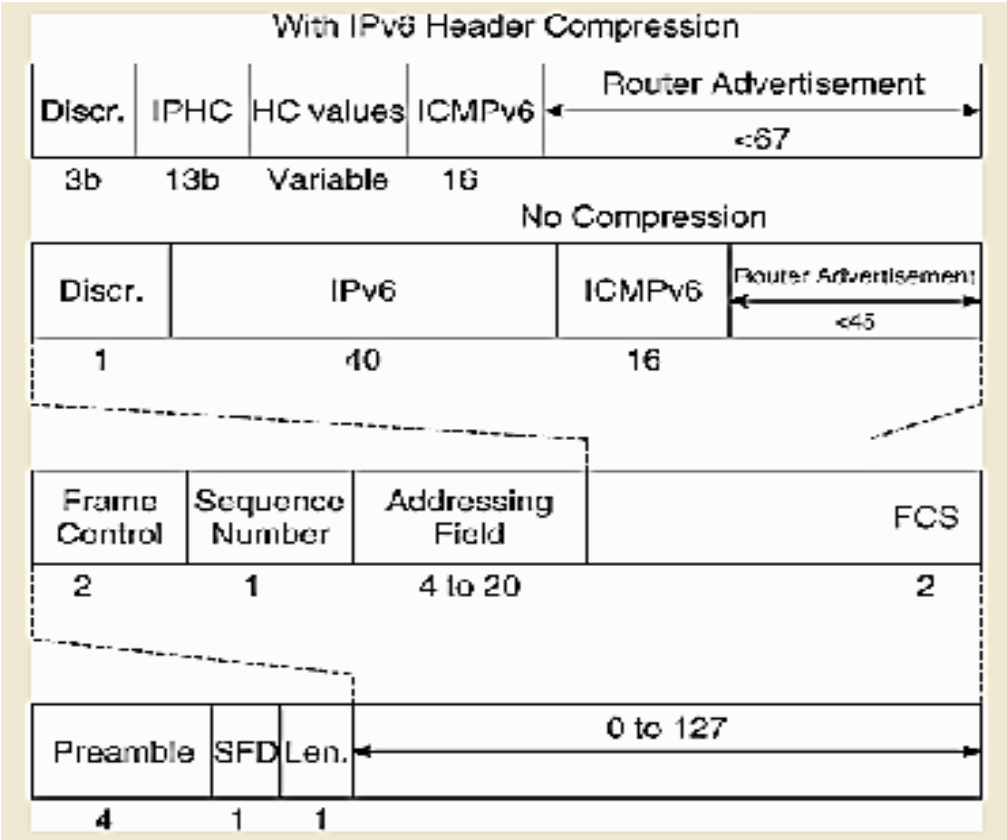

Fig. 4 - Incapsularea in 6LoWPAN [8]

Protocolul permite o marime maxima a datelor de 127 octeti, dar standardul IPv6 impune o valoare minima de 1280 octeti. 6LoWPAN contine un protocol de fragmentare care sa adapteze aceasta contrangere, mai precis ofera un mecanism de compresie a header-ului care reduce lungimea header-ului IPv6, astfel evitand nevoia de a trimite informatie deja cunoscuta sau informatie gasita la nivelul layer-ului retelei de senzori.

Tehnica de compresie definita de standard este inlocuita cu o versiune mai eficienta denumita compresia header-ului IP (IPHC). 6LoWPAN defineste primul octet din campul de date ca un discriminator, care indica cum sunt datele structurate, ca de exemplu:

- 01000001 indica faptul ca bitii ramasi contin un header IPv6 necompresat;
- 011 indica faptul ca header-ul este compresat folosind noua tehnica de compresie;
- 10 indica o incapsulare mesh, adica adresele sursa si destinatie;
- 01010000 contine o eticheta a limitei de propagare a cadrelor broadcast intr-o topologie mesh;
- 11000xxx si 11100xx indica header-ul de fragmentare

Modul in care aceste valori sunt plasate in cadru este fix, pentru a simplifica decodarea. Daca sunt prezente, cadrul trebuie sa inceapa cu header-ul retelei mesh si header-ul de broadcast, urmate de header-ul de fragmentare si in final headerele pentru Layer 3 si Layer 4 (compresate sau nu). Figura anterioara ilustreaza un

exemplu de mesaj cu si fara compresia IPHC, unde in cel mai bun caz valorile de dupa discriminatorul IPHC pot fi reduse la doi octeti, in comparatie cu cei 40 de octeti din header-ul original.

2.1.2 Compresia header-ului in 6LoWPAN - IPHC

Cea mai importanta parte a protocolului este compresia header-ului IPv6 (IPHC).

011	TF	NH	HLIM	CID	SAC	SAM	M	DAC	DAM
3b	2b	1b	2b	1b	1b	2b	1b	1b	2b

Fig.5 - Discriminatorul IPHC [8]

Lungimea fiecarui camp fiind cunoscuta, este usor pentru destinatie sa recupereze valoarea. Eticheta TF (traffic class, flow label) include campul pentru diferite servicii, DSCP (6 biti), notificarea explicita de congestie, ECN (2 biti) si eticheta de flux (20 biti).

Eticheta NH (urmatorul header) specifica cum este procesat protocolul de Layer 4. Daca eticheta este setata pe 0, campul NH este trimis fara modificari catre header-ul IPv6; daca este setat pe 1, o alta eticheta care indica mecanismul superior de compresie poate fi definit dupa valorile header-ului IPHC.

Eticheta limitei hopurilor HLIM (hop limit) defineste cateva valori bine cunoscute in plus fata de valoarea in existenta din retea. Mai exact contextul se refera la un prefix cunoscut de fiecare senzor. Astfel se evita transmiterea valorii prefixului in fiecare header IPHC. Cand eticheta CID este setata pe 1, indica faptul ca 16 contexte pot fi folosite. In acest caz, un extra octet de informatie este adaugat in campul valorii dupa discriminator. Primii patru biti din campul contextului se refera la prefixul sursei iar cei patru biti ramasi la valorile prefixului destinatiei. [8]

Eticheta SAC (source address compression) indica natura prefixului pentru adresa sursei. Eticheta SAM (source address mode) indica nivelul de compresie, ce difera in functie de topologia retelei. O eticheta pentru confirmarea adresei descoperite (DAC) indica daca prefixul este de la o legatura locala sau din context. Daca adresa destinatiei este una multicat, eticheta M este folosita pentru a o diferentia de adresele unicast.

2.1.3 6LoWPAN versus ZigBee

Chiar daca valoarea discriminatorului este selectata pentru a evita posibilele coliziuni cu cadrele de date ZigBee, nu exista inca o metoda fezabila de a distinge pachetele 6LoWPAN de pachetele ZigBee, deci doar unul dintre aceste protocoale ar trebui sa ruleze pe o retea WSN la un moment dat. [5]

ZigBee, la fel ca 6LoWPAN, este creat pentru rate mici de transfer ale datelor si aplicatii ce pot fi sustinute de baterii. ZigBee este in momentul de fata cel mai popular standard de pe piata pentru retele mesh de putere si costuri mici, totodata fiind inca cea mai matura tehnologie folosita in acest domeniu. Este in general implementata pentru retele personale (PAN).

Protocolul ZigBee IP este construit pe baza standardului IEEE 802.15.4, dar spre deosebire de 6LoWPAN, nu poate comunica cu usurinta cu alte protocoale. Singura modalitate de comunicare cu retelele clasice IP este folosirea unui dispozitiv intermediar care sa faca traducerea intre protocoalele folosite de cele doua retele. Acest dezavantaj poate deveni crucial din punct de vedere al evaluarii costurilor si al securitatii retelei. Totodata supervizarea si securizarea legaturii end-to-end devine foarte dificila.

Un beneficiu al ZigBee este totusi faptul ca nodurile pot sta in sleep-mode cea mai mare parte a timpului, permitand o prelungire considerabila a vietii bateriei. Numele tehnologiei provine de la dansul pe care albinele il au in drumul lor pentru lasarea mierii. La fel ca acel dans “haotic”, datele in reteaua ZigBee “sar” dintr-un nod in altul pana cand o ruta catre destinatie este gasita. Rata de transfer a datelor este fixa - 250 kb/s. Aceasta viteza asociata cu puterea mica de transmisie micsoreaza acoperirea retelei ZigBee. De cele mai multe ori sunt necesare repetoare sau o densitate mare de noduri pentru a obtine acoperirea dorita. [5]

2.2 Constrageri de arhitectura si scalabilitate - RPL (Routing Protocol for Low-Power and Lossy Networks)

Implementarea retelelor M2M trebuie sa asigure conectivitatea intre retele din domenii diferite cum ar fi retelele urbane, retelele industriale, retelele din locuinta personala sau cele din constructii. Nici unul dintre protocoalele actuale nu reuseste sa acopere toate cerintele specifice arhitecturii tuturor retelelor enumerate anterior. Protocoalele bazate pe starea legaturii precum OSPF (open shortest path first) sau sistem la sistem precum IS-IS (intermediate system to intermediate system) genereaza o congestie a traficului atunci cand conectivitatea flapeaza. Protocoalele pentru retele ad-hoc precum AODV (ad-hoc on-demand distance vector) sau OLSR (optimized link state routing) nu sunt scalabile pentru un numar mare de noduri senzor.

Protocolul definit de Roll Working Group numit RPL este bazat pe algoritmi cu vectori de distanta, precum protocolul de routare al informatiei RIP, si este creat pentru a corecta probleme de performanta datorate detectarii buclelor eronate (bad loop detection). RPL trebuie sa ramana flexibil si in definirea strategiilor de routare. O retea urbana nu va avea aceleasi constrangeri ca o retea personala si totodata in interiorul fiecarui tip de retea aplicatiile au obiective diferite. De exemplu un sistem de alarma va incerca sa reduca intarzierile de propagare iar o aplicatie ce genereaza mesaje periodice va incerca sa selecteze routerele cu cel mai inalt nivel de energie (cel mai bine alimentate). [7]

2.2.1 Topologie

Topologia RPL este bazata pe grafuri aciclice orientate DODAG (direction oriented directed acyclic graph). DODAG este folosit pentru a permite traficului ce pleaca spre retea sa paraseasca reteaua LLN (low power and lossy network), dar poate fi folosit si dupa pentru a construi o cale inversa catre noduri.

Un singur DODAG poate acoperi intreaga retea LLN dar poate fi alcatuit din mai multe grafuri mai mici. De asemenea mai multe noduri sursa pot fi disponibile in reteaua LLN, precum in figura - nodurile 11 si 51 sunt noduri sursa.

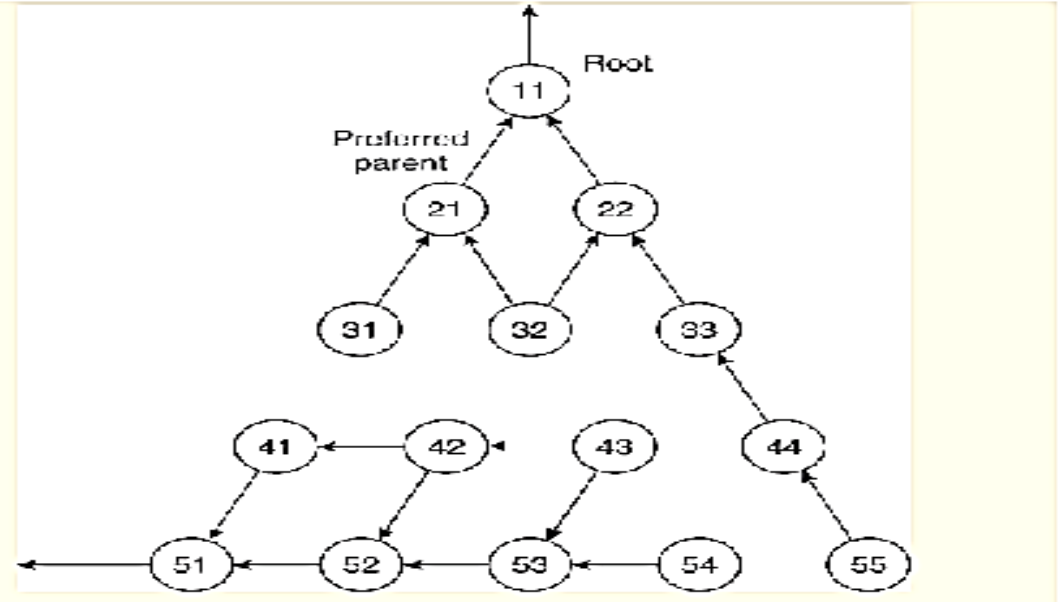

Fig. 6 - DODAG ce contine mai multe grafuri [8]

Nodurile pot folosi diferite instante ale protocolului RPL, ceea ce va conduce la echivalentul unui VLAN, si fiecare instanta va putea folosi diferite constrangeri si diferiti metrici pentru a crea un DODAG. Este relativ usoara construirea diferitelor tabele de routare bazate pe diferitele instante ale DODAG. Pachetele vor trebui sa se deplasese din hop in hop pentru a indica ce instanta a DODAG trebuie folosita. [8]

Uneori nodurile sursa se pot schimba in DODAG. Acest lucru se poate face daca de exemplu anumite inconsistente sunt descoperite in DODAG in urma unor pierderi datorita routerii mesajelor. In acest caz un nou graf DODAG este construit.

2.2.2 Formatul mesajelor si transportul

Nodurile genereaza mesaje de tip DIO (DODAG information object), a caror structura este ilustrata de figura de mai jos. Acest format al mesajului ofera oportunitatea de a intelege cum graful DODAG este construit.

Mesaje de tip DIO sunt trimise periodic pentru a reduce traficul atunci cand reteaua este stabila. DIO pot fi trimise si ca raspuns la DIS (DODAG information solicitation) trimise de alte noduri. Solicitarile DIS pot contine optiuni de limitare a numarului de vecini care pot raspunde.

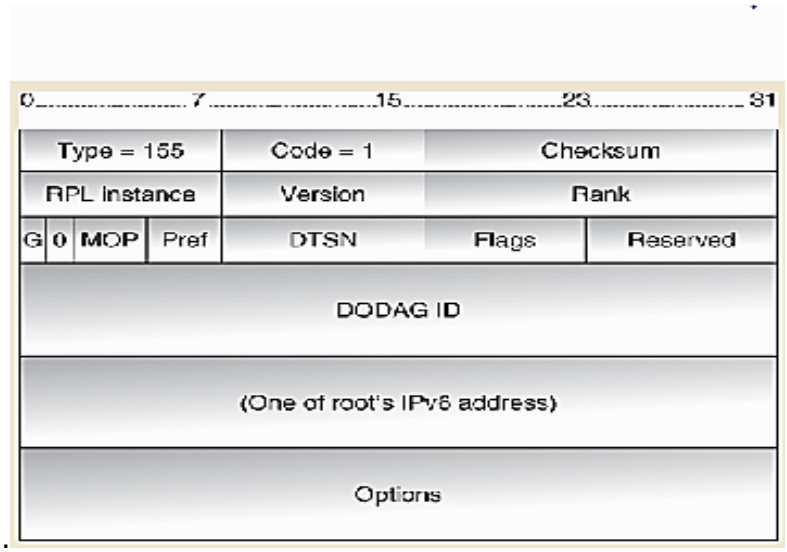

Fig.7 - Formatul DIO [8]

Un nod foloseste mesaje DIO primite de la vecinii lui pentru a le determina rangul si optional alti parametri sau constrangeri. Bazat pe aceasta informatie nodul va selecta un set de posibili parinti si un parinte preferat catre care traficul va fi transmis. Un nod se poate muta usor mai aproape de sursa daca anunturi cu un rang mai bun sunt primite.

Daca un nod trebuie sa isi mareasca rangul, de exemplu atunci cand toti posibilii parinti au disparut, operatia devine mai complexa pentru a minimiza riscul aparitiei unor bucle de routare. Nodul respectiv isi “otraveste” vecinii setand un rang infinit (INFINITE_RANK) in mesajul DIO, care in schimb se rupe de sub-DODAG-ul sursa si devine sursa unui DODAG izolat (floating DODAG). Nodurile care primesc mesajele acestui nod prefera sa fie atasate unui alt parinte cat timp rangul acestuia nu se schimba sau devin si ele izolate si se reataseaza doar de alte noduri izolate.

In directia inversa nodul poate trimite mesaje DAO (DODAG advertisment objects) ca sa isi informeze unii dintre parinti despre adresele accesibile prin el. Mergand catre sursa, acest nod va completa tabelele de routare.

Algoritmul RPL foloseste anumite metrici pentru a crea topologia. Acesti metrici pot fi aditivi (cum ar fi calitatea rutei), pot raporta un minim sau un maxim (energia nodurilor de pe traseu) sau pot fi multiplicativi (rata erorii de pe traseu). Alegerea unui anumit criteriu este independenta de criteriul in sine. De exemplu

calitatea legaturii poate fi vazuta ca un metric aditiv sau ca un metric minim. Metricii si constrangerile pot fi si legate de nod:

- energia: cum este nodul alimentat sau procentul de energie ramasa;
- indicele hop-ului: numarul de hop-uri pe care trebuie sa le parcurga;
- capacitatea si latenta;
- calitatea legaturii;
- ETX (expected transmission): numarul de transmisiuni necesare pentru a trimite cu succes un pachet

3. Optimizarea retelei pentru M2M

Reteaua publica de telefonie actuala nu este creata pentru a suporta aplicatiile M2M. Aceasta a fost creata initial doar pentru traficul telefonic. Chiar dupa introducerea comunicatiilor de date si a retelelor de ultima generatie, acestea nu sunt inca optimizate pentru comunicarea machine-to-machine. Momentan prin intermediul retelelor de telecomunicatii se ofera acces la Internet utilizatorilor, insa transmiterea de date catre un numar urias de dispozitive M2M si oferirea de servicii pentru diferite aplicatii implica o altfel de optimizare a retelei. Arhitectura actuala nu va avea nevoie de o schimbare totala, dar un numar semnificativ de schimbari trebuie implementate pentru a suporta viitoarea piata M2M.

Optimizarile retelei pentru M2M sunt clasificate in cinci categorii:

- reducerea costurilor - costuri scazute pentru operatorii retelelor care vor oferi transfer de date M2M
- servicii cu valoare adaugata - posibilitatea operatorilor sa ofere servicii M2M cu valoare adaugata
- declansarea optimizarilor - oferirea de suport pentru aplicatiilor de retea M2M
- controlul supraincarcarii si al congestiei - asigurarea ca incarcarea produsa de numeroasele aplicatii M2M nu va afecta reteaua
- numirea si adresarea - asigurarea ca vor si suficienti identificatori si adrese intr-o era in care miliarde de dispozitive vor fi conectate

Pentru reducerea costurilor mai multe metode pot fi simultan aplicate precum:

- comunicarea datelor cu aplicatiile M2M se poate face in afara orelor de varf si la costuri mai mici
- reducerea resurselor de retea pentru dispozitive in perioadele in care nu transmit date (dispozitivele M2M au transmit in general date periodic)
- reducerea pe cat posibil a semnalizarii dispozitivelor M2M
- alternativa dezvoltarii unei infrastructuri separate pentru retelele M2M, in ideea separarii informatiilor trimise de dispozitive M2M fata de traficul de date facut de utilizatorii umani

3.1 Identificatori si adresare

Cresterea anticipata a retelei M2M implica mai multe dispozitive si mai multi identificatori necesari. Pentru aceasta problema a numerotarii, identificarii si adresarii numarului tot mai mare de dispozitive ce vor fi legate la retea in perioada urmatoare, au fost propuse mai multe alternative:

1) *IMSI (international mobile subscriber identifier) + adresa IP* -> este o solutie favorabila din punct de vedere al taxarii serviciilor si costurilor pentru ca sistemul este deja implementat in reteaua de telecomunicatii pentru terminalele mobile; principalul dezavantaj ar putea fi securitatea dispozitivului pentru ca identificatorul IMSI nu a fost creat pentru a fi folosit ca un identificator extern, in domeniul public; totodata dispozitive care sa retina asocierea dintre anumiti identificatori si adresa IP a nodului M2M vor fi necesare, precum un server DNS;

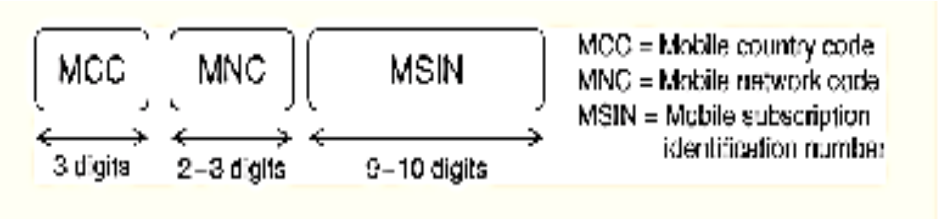

Fig. 8 - Formatul IMSI [8]

Primii 3 biti reprezinta codul tarii, urmatorii 3 codul retelei iar ultimii 9 pot retine maxim 999 999 999 identificatori pentru un operator de telefonie. Tinand cont ca marii operatori au mai mult de 10 milioane de utilizatori si ca reteaua M2M este estimata a avea de 100 de ori mai multi identificatori, folosirea IMSI in actualul format poate fi pusa la indoiala.

2) *IMEI (International Mobile Equipment Identity) si IMEISV (IMEI and software version)* sunt folosite de asemenea la identificarea terminalelor mobile.

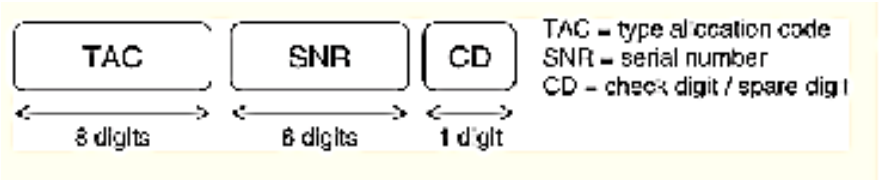

Fig. 9 - Formatul IMEI [8]

IMEI contine codul tipului de alocare (8 biti), numarul de serie (6 biti) si un bit de paritate/rezerva.

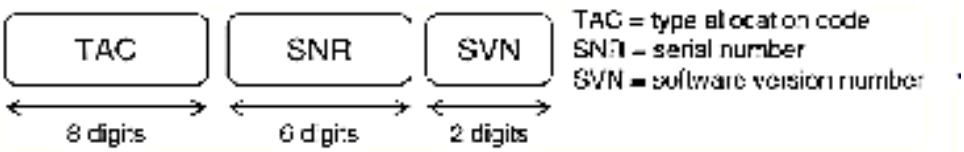

Fig. 10 - Formatul IMEISV [8]

Structura IMEISV este aceeasi cu cea a IMEI, singura deosebire fiind ca in locul bitului de paritate exista doi biti ce identifica versiunea software folosita.
Codul tipului de alocare (TAC) identifica un model particular de dispozitiv mobil. Numarul total de dispozitive ce pot fi identificate cu IMEI este 10^{14} , ceea ce pare adecvat. Cu toate acestea cei mai multi biti sunt ocupati de TAC, numarul maxim de identificatori ramasi fiind de doar un milion. O posibila solutie este totusi alocarea mai multor TAC-uri aceluiasi tip de dispozitiv.

3) *ICCID (International Circuit Card Identifier)*

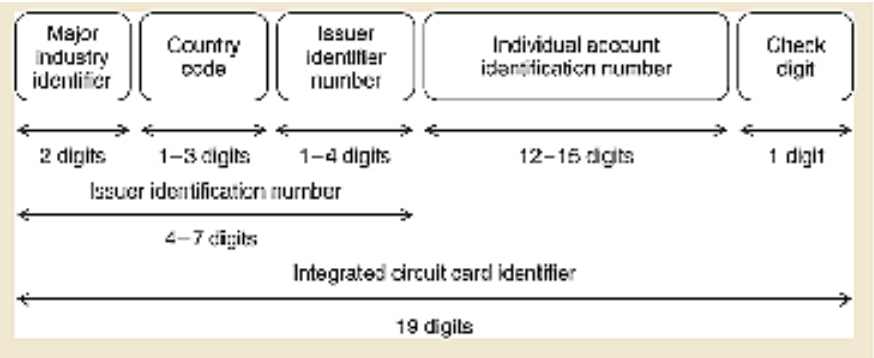

Fig. 11 - Formatul ICCID [8]

ICCID identifica fiecare UICC (Universal Identity Chip Card, cardul ce contine SIM-ul) la nivelul retelei. Cu cel putin 12 biti pentru fiecare identificator de cont personal (Individual account identification number) structura ICCID pare adecvata. [6]

3.2 Controlul congestiei

Supraincarcarea si congestia retelei cauzate de dispozitivele M2M sunt in principal rezultatul unui comportament sincronizat al dispozitivelor M2M care acceseaza simultan reteaua. Principalii factori declansatori ai congestiei ar putea fi:

- aplicatiile M2M care genereaza transmisii recurente de date la intervale de timp sincronizate cu precizie (de exemplu la fiecare ora sau jumatate de ora)

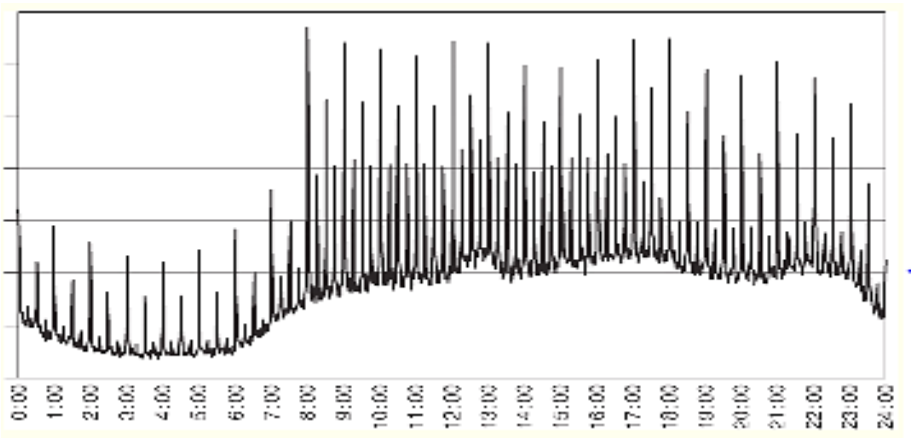

Fig. 12 - Exemplu de acces simultan al aplicatiilor M2M (imagine preluata de la un server) [8]

- un eveniment extern declanseaza conectarea/atasarea unui numar mare de dispozitive M2M in acelasi timp, spre exemplu, un numar mare de dispozitive de masura devin simultan active dupa o perioada in care energia a fost intrerupta
- foarte multi senzori declansati simultan; un exemplu particular este o aplicatie care monitorizeaza un pod: cand un tren traverseaza podul, toti senzorii transmit datele de monitorizare simultan. Acelasi lucru se intampla in monitorizarea hidrologica in timpul perioadelor cu ploi abundente sau in monitorizarea cladirilor atunci cand sunt detectati intrusi;
- o eroare de functionare in aplicatia M2M sau un server, ca de exemplu cand serverul M2M nu confirma primirea datelor trimise de nodurile M2M si acestea continua sa retrimita datele
- multe dispozitive M2M isi pierd acoperirea dupa ce statia telecom la care erau conectate isi intrerupe activitatea; aceste dispozitive M2M vor incerca simultan sa se conecteze la o statie vecina din reteaua mobila;

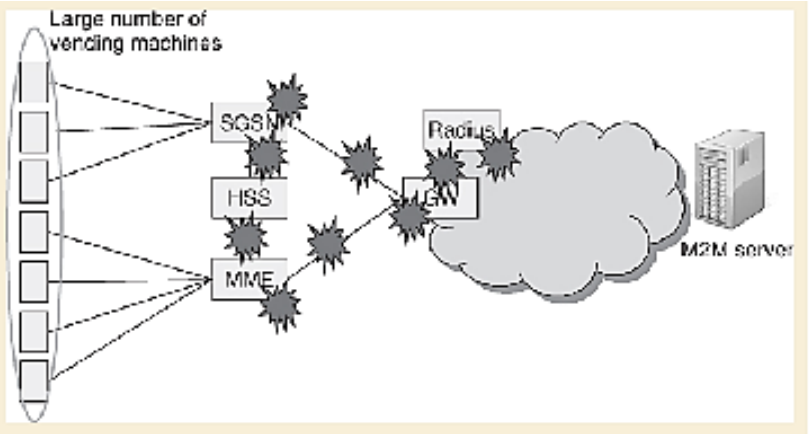

Fig. 13 Congestie de semnalizare a dispozitivelor M2M in reteaua mobila [8]

Controlul supraincarcarii generale si al congestiei sunt necesare pentru a proteja reteaua operatorului de un colaps complet. Mecanismul de protectie are ca obiectiv administrarea incarcarii retelei de catre toate dispozitivele M2M independent de alte dispozitive “traditionale”, si va afecta toate aplicatiile M2M sau o parte semnificativa a acestora. Din moment ce congestia provocata de o aplicatie nu ar trebui sa genereze efecte adverse pentru alte aplicatii M2M, mecanismul de protectie este orientat direct spre acea aplicatie fara a restrictiona traficul non-M2M sau traficul altor aplicatii M2M care nu creeaza probleme.

Rejectarea conexiunilor sau a cererilor de atasare nu ar trebui sa determine dispozitivul M2M sa incerce imediat sa reinitieze aceeasi cerere catre aceeasi retea. Reteaua in sine ar trebui sa devina capabila sa instruiasca dispozitivele M2M sa nu initieze cereri similare decat dupa un timp de revenire. Acest timp de revenire poate

fi de asemenea folosit pentru a pregati dispozitivele M2M cu aplicatii recurente sa isi schimbe programarea dupa care se fac atasarile si cererile de conectare.

5. Concluzii

Dispozitivele si aplicatiile M2M vor deveni tot mai numeroase in anii urmatori reprezentand urmatorul nivel de evolutie al retelei globale - al Internetului. Aparatele electrocasnice si computerul care va controla ambientul casei vor comunica prin intermediul retelelor telecom de ultima generatie.

Mijloacele de transport precum masinile si trenurile vor transmite cantitati uriase de informatie in timpul miscarii. Retelele de senzori vor impanzi orasele masurand atat la suprafata cat si in subteran parametrii retelelor de alimentare cu electricitate sau ai conductelor cu gaz.

Vitezele de conectare, acoperirea si ratele de transfer vor creste exponential. Ideea unei lumi aproape complet conectate ce parea de domeniul science-fiction cu cativa ani in urma incepe sa prinda un contur tot mai clar.

Pentru a crea aceasta lume conectata cu ajutorul dispozitivelor M2M retelele actuale au nevoie de o adaptare la noile cerinte. Contrangerile sunt numeroase si variate: consumul de energie, conectivitatea, securitatea, arhitectura si scalabilitatea, identificarea si adresarea, supraincarcarea vechilor retele sunt doar cateva dintre piedicile ce trebuie depasite, insa avantajele sunt pe masura.

Bibliografie:

[1] https://ro.wikipedia.org/wiki/Internetul_Tuturor_Lucrurilor

[2] https://wfl.ro/tutoriale/ce-este-si-la-ce-serveste-iot-internet-things/

[3] *http://www.zdnet.com/article/m2m-and-the-internet-of-things-a-guide*

[4] https://en.wikipedia.org/wiki/Machine_to_machine

[5] *6LoWPAN vs. ZigBee: https://www.lsr.com/white-papers/zigbee-vs-6lowpan-for-sensor-networks*

[6] *RPL: http://cnds.eecs.jacobs-university.de/courses/nds-2010/kuryla-rpl.pdf*

[7] *The Internet of Things: Key Applications and Protocols, 2nd Edition*
Olivier Hersent, David Boswarthick, Omar Elloumi
John Wiley & Sons, 2012

[8] *M2M communications – A System Approach – David Boswarthick, Omar Elloumi, Olivier Hersent, Editura john Wiley and Sons, 2012*