UTILIZAREA DISPOZITIVELOR INTERNET OF THINGS (IOT) ÎN VEDEREA MONITORIZĂRII DE LA DISTANȚĂ A TRADUCTOARELOR DE NIVEL MONTATE ÎN REZERVOARE INDUSTRIALE

Drd. ing. Dorin BUIUM, Conf. dr. ing. Mariana FRATU

Universitatea „Transilvania” din Brașov, Facultatea de Inginerie Electrică și Știința Calculatoarelor, Brașov, România

REZUMAT: Producerea dispozitivelor interconectabile exploatează tehnologii de dată recentă, neexplorate suficient, iar proiectarea lor impune mai multe aspecte legate de tehnologii în expansiune și de securitate.

CUVINTE CHEIE: Internet, internetul obiectelor, rețea de obiecte, interconectare, securitate.

ABSTRACT: The production of interconnectable devices exploits recent, unexplored technologies, and their design imposes several aspects related to expanding and security technologies.

KEYWORDS: Internet, Internet of Things, network of things, network, security.

1. INTRODUCERE

Internetul obiectelor (în engleză Internet of Things, abreviat IoT) este un concept ce presupune folosirea internetului pentru a conecta între ele diferite dispozitive, servicii și sisteme automate, formând astfel o rețea de obiecte.

IoT reprezintă rețeaua de obiecte fizice - „lucruri” - care conțin senzori, software și alte tehnologii, în scopul conectării și schimbului de date cu alte dispozitive și sisteme de pe internet. Aceste dispozitive pot fi de la simple obiecte de uz casnic până la unelte industriale sofisticate. În prezent, există peste 10 miliarde de dispozitive conectate la IoT, dar experții se așteaptă ca acest număr să crească la 22 de miliarde până în 2025. Oracle are o rețea de parteneri de dispozitive.

IoT industrial (IIoT) se referă la aplicarea tehnologiei IoT în medii industriale, în special pentru instrumentarea și controlul senzorilor și dispozitivelor care interacționează cu tehnologiile cloud. Un exemplu bun de utilizare a IIoT este cazul Titan. Citiți fișierul PDF. Recent, industriile au început să utilizeze comunicarea machine-to-machine (M2M) pentru a obține automatizare și control wireless. Dar, odată cu apariția tehnologiilor cloud și a celor conexe (cum ar fi analizele și machine learning), industriile pot atinge un nivel superior de automatizare, creând astfel noi venituri și modele de afaceri. IIoT este denumit uneori cel de-al patrulea val al revoluției industriale (sau Industry 4.0).

Aplicațiile IoT utilizează algoritmi de "machine learning" pentru a analiza cantități masive de date de la senzorii conectați în cloud. Datorită dash-boardurilor și alertelor IoT în timp real, se obține vizibilitate asupra principalilor indicatori de performanță, statisticilor privind perioada medie dintre eșecuri și alte informații. Algoritmii bazați pe machine learning pot să identifice anomaliile la echipamente și să trimită alerte către utilizatori sau chiar să declanșeze acțiuni automate de corecție sau de prevenție.

Cu aplicațiile IoT bazate pe cloud, utilizatorii business pot îmbunătăți rapid procesele existente pentru lanțurile de aprovizionare, serviciile pentru clienți, resursele umane și serviciile financiare. Nu este nevoie să creați procese de business întregi.

In functie de modul de functionare, dispozitivele din reteaua IoT se impart in trei tipuri diferite:

– dispozitive care colecteaza informatia si o transmit mai departe altor dispozitive sau utilizatorului;

– dispozitive care primesc informatii de la alte dispozitive sau de la utilizator si actioneaza în consecință;

– dispozitive care îndeplinesc ambele funcții descrise mai sus.

2. CONECTAREA SENZORILOR PRIN IOT

Utilizarea dispozitivelor conectate la internet presupune colectare de date, procesare de date și

generarea unui răspuns. Pentru a îndeplini aceste funcții, sistemele inteligente au nevoie în primul rând de senzori. Aceștia adună date și "traduc" pentru dispozitive starea lumii înconjurătoare.

Scopul lor este unul simplu: măsurarea și detectarea schimbărilor de mediu. Dacă acționează independent, senzorii singuri nu au un impact considerabil. Însă raportarea datelor pe care le colectează transformă senzorii în cercetași pe care dispozitivele inteligente îi folosesc pentru a înțelege teritoriul fizic și pentru a-l modifica la parametri prestabiliți.

Aceste mici elemente de tehnologie reprezintă prima linie de automatizare și au un rol esențial în ecosistemul IoT. Senzorii pot fi grupați pe același dispozitiv inteligent care declanșează acțiunea sau pot transfera datele către un aparat mult mai complex. Indiferent de modul în care sunt integrați, senzorii sunt cei care pun la lucru un dispozitiv conectat.

Senzorii sunt peste tot în jurul nostru. Spre exemplu, telefoanele inteligente includ un număr mare de senzori pentru a stabili poziția (GPS, giroscop), viteza (accelerometru), proximitatea, lumina ambientală, vocea, atingerea, amprenta digitală, presiunea aerului (barometru), umiditatea sau temperatura dispozitivului și a încăperii. Un telefon obișnuit integrează aproape toți acești senzori pentru a furniza date către aplicații.

Senzorii sunt utilizați într-o gamă largă de domenii. Ei automatizează diferite sarcini pentru a spori eficiența unui sistem și pentru a diminua costurile. În agricultură, sunt utilizați pentru a verifica pH-ul solului își nivelurile de umiditate; în mediile industriale, senzorii ajută la detectarea substanțelor chimice sau a radioactivității; calitatea aerului este, de asemenea, monitorizată prin intermediul acestor mici dispozitive.

Senzorii optici care măsoară calitatea razelor de lumină sunt utilizați pentru a declanșa diferite acțiuni: de la pornirea automată a unei camere de supraveghere de acasă la detectarea mișcării .

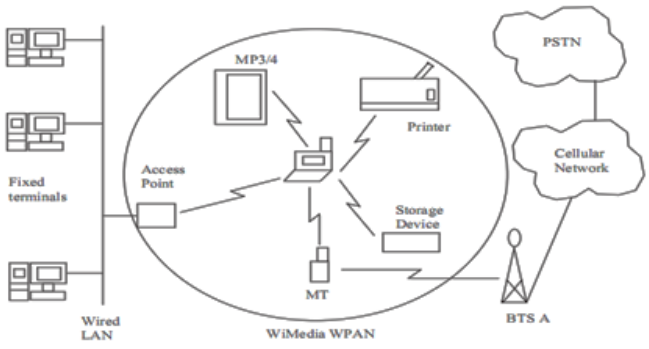

Fig. 1 Elementele componenete ale ecosistemului IoT.

Mai simplu, senzorii sunt punctul de contact între dispozitivul inteligent și mediul real pe care dorește să îl influențeze pentru ca deținătorul să se simtă mai confortabil.

3. RETELE DE SENZORI IOT

O rețea de senzori *IoT* este o colecție de noduri senzor ce formează o rețea temporară care furnizează informații fără sa fie nevoie să o administrăm și fără a-i oferi drept suport servicii.

Cu alte cuvinte, nu este o structură fixă. În general nodurile senzor folosesc dispozitive emițătoare-receptoare wireless de radio-frecvență, pe post de interfață de reăea, iar comunicația între noduri este realizată folosind legaturi wireless multi-hop. Fiecare nod din rețea se comportț ca un router, rutând pachete pentru nodurile vecine. Asemănător cu rețelele ad-hoc, trebuie să facă față la schimbări frecvente de topologie. Aceasta se întamplă deoarece nodurile senzor sunt predispuse eșecurilor și de asemenea noduri noi se pot alatura rețelei și astfel se poate compensa apariția nodurilor defecte și se poate chiar maximiza eficiența rețelei. Datorită acestor caracteristici o problemă esențială în proiectarea unei rețele de senzori este dezvoltarea unei structuri de senzori cu posibilități de auto-organizare și cu protocoale de rutare dinamice care să gasească rutele cele mai eficiente pentru comunicarea între nodurilel rețelei.

Pentru senzorii mici, concepuți pentru a se coordona în scopul realizării unei detecții considerabile, cu consum de energie mic, aceștia trebuie să lucreze în grup (cluster). În fiecare grup, un nod este desemnat ca fiind conducătorul grupului pentru a se ocupa de administrarea celorlalte noduri ale grupului.

Avantajele organizării de/pe grupuri:

– gruparea le permite senzorilor posibilitatea de a-și coordona în mod eficient interacțiunile locale pentru realizarea/atingerea unui obiectiv global.

– scalabilitatea;

– crește robustețea rețelei;

– utilizare mai eficientă a resurselor;

– consum mai mic de energie.

Serviciile din nivelul de servicii includ, printre altele, protocoale de rutare, distribuirea și acumularea datelor. Nivelul fizic se referă în mod fizic la nodurile rețelei, care pot fi noduri fiu, noduri conducatoare de grup, noduri părinte (noduri conectate la două sau mai multe noduri conducătoare de grup). Mesajele din rețea sunt modelate virtual la nivelul de date.

Atunci când se produce/sesizeaza un eveniment, nodurile sink emit o cerere de tip broadcast, fie întregii rețele, fie spre o regiune anume a rețelei, în funcție de tipul cererii. Când nodurile (senzorii) – apropiate de evenimentul/obiectul ce trebuie detectat – detectează spre exemplu o schimbare de temperatură, poziție,

viteză, etc., fac un broadcast cu aceste date către toate nodurile vecine. Sarcina conducătorilor de grup este de a procesa și a acumula informație și apoi să facă un broadcast către nivelele superioare prin intermediul nodurilor vecine. Deoarece nodurile conducător de grup primesc numeroase informații de la nodurile din grup acestea trebuie să proceseze și să filtreze aceste informații.

În rețelele de senzori pentru a compensa limitările hardware în ceea ce privește memoria disponibilă, bateria și puterea de calcul, aplicațiile cu rețele de senzori dispun de un numar mare de senzori în zona de interes. Acești senzori colaborează între ei comportându-se ca o mare rețea wireless ad-hoc. Distanța mică dintre noduri ajută, deasemenea, la economiserea energiei – informația străbate distanțe mai mici.

Prima etapă a unui sistem IoT se referă la partea fizică a IoT-ului și anume la dispozitivul de detectare ce adună date din împrejurimi și care este bazat pe o anumită funcție. Spre exemplu senzori atmosferici, de nivel, de presiune, de lumină, etc.

După ce datele au fost culese merg către a doua etapă și anume etapa de conectivitate ce se realizează cu ajutorul internetului, iar datele culese ajung intr-un cloud. Conectivitatea are loc, de obicei, prin una din metodele următoare: wi-fi, bluetooth, RFID, NFC, etc.

După aceea datele merg în etapa de procesare unde are loc analiza datelor prin diverși algoritmi.

Ultima etapa este etapa pe care toți o vedem și se referă la interfața device-ului cu care noi interacționăm și unde ne este arătat răspunsul final.

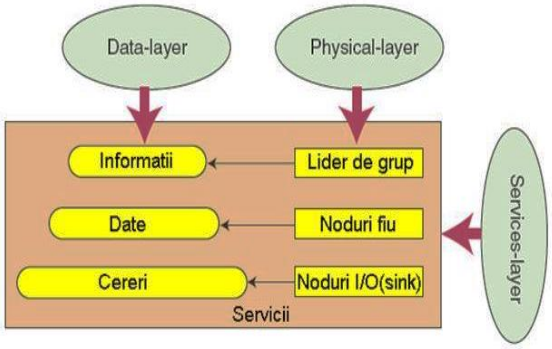

Fig. 3 Arhitectura IoT cu retele de senzori.

Producătorii pot obține un avantaj competitiv utilizând monitorizarea liniei de producție pentru a permite întreținerea proactivă a echipamentelor atunci când senzorii detectează o defecțiune iminentă. Senzorii pot măsura de fapt când producția este compromisă. Cu ajutorul alertelor senzorilor, producătorii pot verifica rapid echipamentul pentru acuratețe sau îl pot scoate din producție până când este reparat. Acest lucru permite companiilor să reducă costurile de operare, să obțină un timp de funcționare mai bun și să îmbunătățească gestionarea performanței activelor.

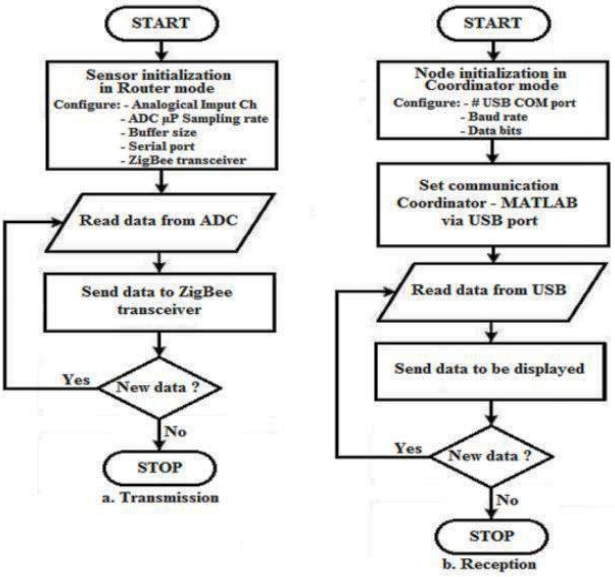

Fig. 2. Schema logică de comunicare a unui senzor in retea.

4. SISTEMUL GSM FOLOSIT IN TEHNOLOGIA IOT

Sistemul GSM este alcîtuit din trei segmente majore: stația mobila (MS), subsistemul stației de baza (BSS), subsistemul de retea si de comutare (NSS).

MS preia informația de la utilizator și o prelucrează, conform protocoalelor de transmisie aflate în atmosfera, pentru a putea realiza transferul la BSS. Informația este transmisă de utilizator la MS prin intermediul unui microfon sau difuzor, tastatură, afisaj pentru mesaje scurte, iar între celelalte terminale transmisia se realizează prin cablu. MS are doua elemente: echipamentul mobil (ME) și Subscriber Identity Module (SIM). ME este un dispozitiv hardware, pe care clientul îl poate procura de la producător sau de la diverși dealeri. Acesta contine toate componentele necesare implementării protocoalelor ce asigură interacțiunea cu utilizatorul, pe de o parte, cât și cu canalul de frecvență prin care ajunge la BSS. Componentele includ microfon, difuzor, tastatură și modemul radio. SIM este smart card, eliberat pe baza de abonament și variind în funcție de preferințele utilizatorului. Apeluriile sunt direcționate mai degrabă la SIM, și nu la terminal. De asemenea, mesajele sunt și ele stocate în SIM. Întrucât cardurile SIM păstrează informațiile personale ale utilizatorului s-a introdus o măsură de securitate ce constă în introducerea unui număr PIN de patru cifre de către utilizator.

BSS comunică cu utilizatorul prin wireless și cu infrastructura cablată prin intermediul protocoalelor wired. Cerințele pentru cele două medii, wireless si cablat, sunt diferite întrucât mediul wireless este nesigur, cu o lățime limitată a benzii și trebuie să

asigure mobilitate. Drept rezultat, protocoalele folosite de cele două medii sunt diferite. BSS este cel care asigură traducerea între cele două protocoale, astfel: în cazul unei conversații, semnalul de voce al utilizatorului este convertit în semnal digital de 13kbps, cu ajutorul unui decodificator de voce, destul de redus pentru a se încadra pe canalul de frecvență din atmosferă.

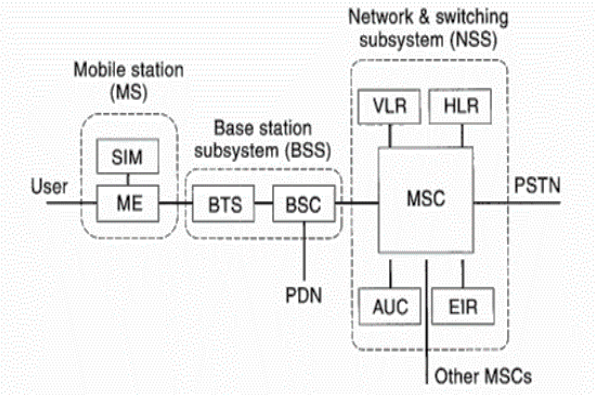

Fig. 4. Elementele componenete ale sistemului GSM

Această conversie, de la analog la digital, are loc la nivelul MS-ului. Întrucât rețeaua backbone lucrează cu 64kbs, se realizeză conversia de la 13kbps la 64kbps, aceasta realizându-se în cadrul BSS-ului. În cadrul BSS-ului se găsesc doua elemente: BTS și BSC. BTS este partea din cadrul MS-ului care comunică fizic cu interfața aerului. Componentele BTS-ului includ un emițător, un receptor și echipament de semnalizare pentru a comunica cu interfața aerului. BTS-ul este localizat în centrul celulelor, unde este instalată antena BSS, și pot exista de la 1 la 100 de astfel de BTS-uri în cadrul unei singure BSS. Cel de-al doilea element arhitectural al BS-ului este BSC-ul, un mic comutator care are drept responsabilitate administrarea frecvenței și realizează predarea semnalului țntre BTS-uri.

NSS este responsabil pentru funcționarea rețelei, furnizând comunicarea cu alte rețele wireless sau cablate. NSS-ul folosit de GSM se conectează cu PSTN (rețeaua backbone) cu ajutorul protocoalelor ISDN. NSS poate fi considerat ca fiind un comutator wireless care comunică cu alte comutatoare ale rețelei backbone și, în același timp, suportă funcționalitățile necesare unui mediu celular mobil. NSS-ul este cel mai elaborat element din cadrul rețelei GSM, având un hardware (MSC) și patru componente software: visitor location register (VLR), home location register (HLR), equipment identification register (EIR), authentication center (AUC). MSC este partea hardware a comutatorului NSS, ce comunică cu comutatoarele rețelei backbone, prin intermediul protocolului SS-7 (signaling system-7), precum și cu alte MSC-uri aflate în aria de acoperire a furnizorului de servicii. De asemena, MSC furnizează rețelei informații cu privire la statutul terminalelor mobile. HLR este baza de date care realizează mangementul contului fiecărui abonat mobil. Aici se pastrează adresa abonatului, tipul serviciului, locația curentă, adresa de expediere, codurile de autentificare, precum și informații de facturare. VLR este o bază de date temporară, similară cu MSC, identificând utilizatorii care vizitează zona de acoperire a unui MSC. Intreținerea a doua baze de date face posibilă apelarea și rutarea apelurilor într-o situație de roaming, atunci când un MS pătrunde în zona de acoperire a altor MSC-uri. AUC păstrează algoritmi diverși utilizați în autentificarea sau criptarea abonaților. EIR este o altă bază de date care gestionează identificarea echipamentului mobil în caz de furt sau defecte. Această bază pastrează identitatea internațională a echipamentului mobil (IMEI) care dezvăluie producătorul, țara de producție și tipul terminalului, informație ce poate fi folosită pentru a raporta telefoanele furate. Implementarea EIR este optionala.

5.CONCLUZII

Progresul comun al microelectronicii, microtehnologiei , tehnologiilor de transmisie fără fir și aplicațiilor software a făcut posibilă producerea la un cost rezonabil de micro-senzori de câțiva milimetri cubi în volum, capabili să funcționeze în rețele.

Comunicarea în timp real prin intermediul platformelor dedicate va usura dezvoltarea și mentenanta în toate domeniile de activitate, urmând ca în viitorul apropiat, „Internet of Things” să devină un lucru cotidian.

Tot ce este nou și complex are si dezavantaje, iar securitatea și protecția vieții private sunt cele mai mari provocări pentru IoT.

Aparatele si dispozitivele folosite colectează date personale despre utilizatori – echipamentele inteligente „stiu”când sunteți acasă, ce produse electronice si electrocasnice folositi, tipul de transmisie de date utilizat, setarile operationale efectuate cât și alte date care vor fi deținute împreună cu cele ale altor echipamente similare, în bazele de date a companiilor furnizoare de servicii de livrare/ instalare/ operaționalizare/ mentenanță.

Experții de securitate susțin că nu se face suficient pentru a construi un mediu integrat de securitate și confidențialitate în IoT, la aceste stadii incipiente.

Pentru a demonstra riscul utilizării acestui sistem, aceștia au „piratat” o serie de dispozitive sau sisteme, de la monitoare instalate pentru supravegherea copiilor conectate la iluminare automată la frigidere, aparate inteligente, precum și sisteme imporatante ale orașului

cum ar fi semnalele de trafic, camere de supraveghere, etc.

Hackerii nu desfasoară încă activități importante în acest domeniu, deoarece nu este încă suficient de dezvoltat și implementat, dar supraveghează cu mare atenție IoT:

– deocamdată nu sunt, probabil, suficient de mulți utilizatori care folosesc obiecte conectate spațial unei case inteligente, pentru a merita efortul unui atac împotriva lor, dar ca întotdeauna, de îndată ce există un beneficiu pentru hacking, va exista un cyber criminal gata de acțiune.

– se constată necesitatea instrurii utilizatorilor de IoT, pentru a înțelege valoarea interconectării echipamentelor versus risc expunere la pierderea controlului acestora și/sau furnizarea în cyberspațiu a unor informații comporatmentale private.

– este responsabilitatea entităților de digitalizare a lumii noastre fizice, de a educa, proteja și a ajuta la promovarea de noi precedente, avand în vedere că aceste entități sunt responsabile de comportamentul societății fata de IoT.

BIBLIOGRAFIE

[1] https://despretot.info/internet-of-things-iot-definitie-dex/

[2] http://www.wall-street.ro/tag/internet-ofthings.html#ixzz48qK2SHgc

[3] I.P. Zarko, K. Pripuzic, M. Serrano, „Interoperability and Open-Source Solutions for the Internet of Things”

[4] https://www.theguardian.com/technology/2015/may/06/whatis-the-internet-of-things

[5] A. McEwen, H. Cassimally, „Designing the Internet of Things”

Despre autori

Drd. Ing. Dorin BUIUM
Universitatea „Transilvania” din Brașov, Romania

Drd.Ing.Dorin Buium este absolvent al Universității „Transilvania” din Brașov, promitia (2015), Energetica, master în Sisteme automate avansate și tehnologii informatice (2017), doctorand in cadrul Facultatii de Inginerie Electrica si Stiinta Calculatoarelor, departamentul Automatica si Informatica aplicata (2019- prezent). Din anul 2016 a lucrat în domeniul automatizărilor din industria alimentară în companii din Brașov. In cadrul acestor companii a participat la proiecte de montare a liniilor de fabricatie, precum si de modernizare a instalatiilor de procesare, depozitare, transfer, dozare si îmbuteliere. Domeniile de competenta sunt: automatizări în instalații de producere și distribuție utilități (electricitate, instalații termice, instalații frigorifice, aer comprimat, lichefiere gaze),precum și sisteme SCADA pentru monitorizarea consumului de utilitați și creșterea eficienței energetice.

Dr. Ing. Mariana FRATU
Universitatea „Transilvania” din Brașov, Romania

Mariana Fratu a absolvit Facultatea de Inginerie Electrică din cadrul Universității Brașov, România, în 1982. S-a alăturat Departamentului de Instalații pentru Construcții al Universității „Transilvania”din Brașov, România, în 1978, iar în prezent este profesor asociat la Departamentul de Instalații pentru Construcții. A obținut titlul de doctor în sisteme electrice de la aceeași universitate în 2008. Este autoarea a cinci cărți, a peste 100 de articole și a unei invenții. Interesele sale actuale de cercetare includ controlul inteligent al clădirilor, sisteme discrete, prototipuri virtuale și simulare.