Vilniaus universitetas
Matematikos ir informatikos institutas
L I E T U V A

INFORMATIKOS INŽINERIJA (07 T)

MULTIMODALINIO DAIKTŲ INTERNETO OBJEKTŲ IDENTIFIKAVIMO IR AUTENTIFIKAVIMO METODO TYRIMAS IR TOBULINIMAS

Raimundas Savukynas

2017 m. spalis

Mokslinė ataskaita **MII-DS-07T-17-18**

VU Matematikos ir informatikos institutas, Akademijos g. 4, Vilnius LT-08663

www.mii.lt

Santrauka

Mokslinėje ataskaitoje apžvelgiama mokslinių tyrimų literatūra daiktų interneto ir objektų identifikavimo tema. Daiktų interneto resursai ir teikiamos paslaugos yra pasiskirsčiusios informaciniame tinkle, todėl būtina turėti mechanizmą leidžiantį identifikuoti ir atrasti išmaniuosius įrenginius, jų teikiamas paslaugas ir resursus. Paprastai identifikacija susideda iš vardų priskyrimo resursams ir resursų adresavimo mechanizmo tam, kad atrasti ir pasiekti nutolusius daiktų interneto resursus. Šiuolaikiniuose tinkluose naudojami DOI (angl. *Digital Object Identification*) ir URI (angl. *Universal Resorce Identifier*), kurie identifikuoja resursą, jo tipą bei aibę lygiaverčių vardų. Jie leidžia identifikuoti fizinius objektus, esančius bet kurioje pasaulio vietoje panaudojant EPC (angl. *Electronic Product Code*) technologiją. EPC leidžia DOI ir URI panaudoti kartu su RFID (angl. *Radio-Frequency Identification*). RFID technologija skirta objektų žymėjimui ir sekimui, paremta radijo dažnio signalo panaudojimu objekto žymoje esančios informacijos įrašymui ir nuskaitymui.

Reikšminiai žodžiai: daiktų internetas, objektų identifikavimas, ateities internetas, interneto paslaugos, išmanieji įrenginiai.

Tyrimo objektas

Išmaniosios daiktų interneto aplinkos ir daiktų interneto objektų identifikavimo ir autentifikavimo metodai.

Tyrimo tikslas

Sukurti heterogeniškų daiktų interneto įrenginių decentralizuotus identifikavimo ir autentifikavimo metodus, skirtus transporto išmaniosioms aplinkoms.

Tyrimo uždaviniai

1. Apžvelgti daiktų interneto architektūros ir jos elementų savybes, skirtas identifikuoti įvairių rūšių objektus ir paslaugas per internetą.
2. Išanalizuoti daiktų interneto komunikacijos protokolus ir standartus, skirtus identifikuoti išmaniuosius įrenginius, jų teikiamas paslaugas ir resursus.
3. Išnagrinėti ir palyginti daiktų interneto objektų identifikavimo metodus, kurie leistų atrasti vienas nuo kito nutolusius objektus ir paslaugas.

Turinys

1. Įvadas

Išmaniųjų įrenginių apsuptis ir internetas tapo įprastu reiškiniu mūsų gyvenime. Daugumoje gyvenimo sričių ir ūkio sektorių, valdymas ir stebėjimas vyksta naudojant internetą, o taip pat įvairius skaitmeninius įrenginius sąveikaujančius per tinklą. Duomenys tinklu perduodami ne tik naudojant „žmogus ir žmogus“ arba „žmogus ir kompiuteris“ sąveikas, bet ir per jutiklius tarpusavyje sąveikaujant įrenginiams, kurie dar yra vadinami interneto daiktais. Taip susiformavo daiktų internetas (angl. *Internet of Things – IoT*), kuris yra nauja tinklų konfigūracija, apimanti fizinių objektų komunikavimą ir objektų bei žmonių sąveiką internete. Daiktų internetas dažnai yra vadinamas kita interneto evoliucijos pakopa, kur daiktai tampa aktyvūs verslo, informacijos ir socialinių procesų dalyviai, galintys komunikuoti ir sąveikauti tarpusavyje, o taip pat su juos supančia išmaniąja aplinka keisdamiesi duomenimis, autonomiškai reaguoti į fizinio pasaulio įvykius bei įtakoti aplinką, atliekant įvairius veiksmus ir teikiant paslaugas. Išmaniųjų aplinkų ir daiktų interneto teikiami privalumai apima komforto, saugumo, energetinių išteklių optimalaus panaudojimo ir daugelį kitų paslaugų, kurios gerokai pagerina gyvenimo kokybę. Daiktų interneto panaudojimo galimybės neapsiriboja vien tik teikiamomis paslaugomis žmonėms, bet leidžia pritaikyti įvairias technologijas pramonėje, prekyboje, švietime, transporte ir netgi skaitmeninėje realybėje, kur tarpusavyje komunikuoja ir sprendimus priima išmanūs programiniai agentai (Gubbi *et al*. 2013).

Daiktų internetas yra pasaulinis daiktų, turinčių sąsajas su jutikliais, valdikliais, programine įranga bei gebančių surinkti, apdoroti ir keistis įvairia informacija tinklas, kurio veikimas grindžiamas šiuo metu esamų ar visiškai naujai vystomų informacijos ir komunikacijos technologijų tarpusavio sąveika. Daiktų interneto kontekste daiktu laikomas fizinio arba informacijos pasaulio objektas, kuris gali būti identifikuotas ir įjungtas į komunikacinius tinklus. Kiekvienas objektas turi elektroninę žymą (angl. *Electronic Tag*) ir nuolat prijungtas prie duomenų bazės bei tinklo, todėl tokius objektus galima nesudėtingai kontroliuoti ir valdyti. Fiziniai objektai paprastai egzistuoja fiziniame pasaulyje, o informacija apie juos gaunama per stimuliuojamus ir sujungiamus jutiklius. Toks fizinis objektas, kuris įgauna komunikavimo savybes, gali jungtis į daiktų internetą. Fiziniu objektu gali būti mus supančios aplinkos dalis, kuri fiziškai sąveikauja su kitais daiktais, žmonėmis ar aplinkomis. Informacijos objektai paprastai egzistuoja informaciniame pasaulyje ir gali būti saugomi, tvarkomi ir

naudojami. Toks informacijos objektas veikia išmaniojoje aplinkoje, naudoja išmaniąsias sąsajas ir turi unikalius identifikacijos atributus, kurie leidžia jį skaitmeniškai personalizuoti. Informacijos objektu gali būti skaitmeninis elementas turintis konkretų tikslą, sudarytas iš duomenų eilučių ir galintis atlikti nustatytus veiksmus. Fizinį objektą informacijos pasaulyje gali atstovauti vienas ar daugiau informacijos daiktų, o informacijos objektas gali egzistuoti ir be jokio kartu susijusio fizinio daikto (Espada *et al*. 2011).

Daiktų internetas yra suprantamas kaip informacinei visuomenei skirta pasaulinė infrastruktūra, teikianti šiuolaikines paslaugas, sujungiant objektus jau esamų ir naujai besivystančių informacinių bei komunikacinių technologijų pagrindu. Identifikuojant, renkant duomenis, juos apdorojant ir naudojantis komunikacijų galimybėmis, daiktų internetas leidžia panaudoti objektus įvairioms paslaugoms, užtikrinant aukštus saugumo ir privatumo reikalavimus. Daiktų interneto pagalba tikimasi sujungti į visumą naujausias technologijas kaip šiuolaikinė mašina – mašinai (angl. *Machine to Machine* – M2M) komunikacija, autonominiai tinklai, duomenų analizė ir sprendimų priėmimas, saugumo ir privatumo apsauga, debesų kompiuterija su moderniomis pojūčių ir paleidimo technologijomis. Pagrindiniai daiktų interneto požymiai (Nitti *et al.* 2016):

- sujungiamumas: viskas gali būti sujungta su pasaulio informacijos ir komunikacijų infrastruktūra;
- susiejamumas: daiktų internetas gali teikti su objektais susijusias paslaugas, atsižvelgiant į apribojimus kaip privatumo apsauga ir semantinė darna tarp fizinių ir informacijos objektų;
- heterogeniškumas: daiktų interneto objektai gali būti nevienalyčiai, nes remiasi absoliučiai skirtingomis technologinėmis platformomis ir tinklais;
- dinamiškumas: objektų būsena gali keistis dinamiškai, nes jie užmiega ir atsibunda, įjungiami arba išjungiami, o taip pat keičiasi jų vieta ir greitis;
- mastas: valdomų ir tarpusavyje komunikuojančių objektų skaičius bus daug kartų didesnis nei prie dabartinio interneto prijungtų įrenginių skaičius.

Daiktų interneto kūrimas priklauso nuo daugelio inovacinių technologijų, bet pirmiausia nuo jutiklių, mobilių įtaisų, bevielio tinklo, nanotechnologijų ir standartinio interneto. Daiktų internetą galima laikyti ateities technologijų vizija, kai realaus pasaulio objektai tampa interneto sudėtine dalimi, kur kiekvienas objektas yra tiksliai identifikuojamas, nustatoma jo vieta ir būsena. Šios naujos paslaugos ir jų išmanumas

kelia daiktų interneto technologijoms aukšto lygio reikalavimus (Kraijak *et al.* 2015):

- identifikuotas ryšys: daiktų internetas turi užtikrinti komunikaciją tarp objekto ir daiktų interneto, paremtą pagrindiniais daikto identifikatoriais, o taip pat apimti galimą skirtingų daiktų identifikatorių įvairiarūšiškumą, kurie būtų tvarkomi vienodai;
- autonominis aprūpinimas: daiktų internetas turi suteikti paslaugas, kurias būtų galima pateikti užfiksuojant, perduodant ir automatiškai apdorojant objektų duomenis, kurie grindžiami taisyklėmis ir sukonfigūruoti operatorių, o tuo pačiu priklauso nuo automatinės duomenų sintezės ir jų gavybos;
- interoperabilumas: daiktų internetas turi apimti sąveiką tarp įvairiarūšių ir išskirstytų sistemų, naudojantis skirtinga informacija ir paslaugomis;
- autonominis tinklas: daiktų internetas turi įgalinti visiškai savarankišką tinklą, siekiant prisitaikyti prie skirtingų taikomųjų sričių, komunikacijos aplinkų, didelio įrenginių skaičiaus ir skirtingų jų tipų;
- vietos nustatymas: daiktų internetas turi naudoti objektų buvimo vietos nustatymo galimybes, nes komunikacijos ir paslaugos priklauso nuo objektų padėties informacijos, kurią gauti gali varžyti šalies įstatymai, teisės aktai arba saugumo reikalavimai;
- saugumas: daiktų internetas turi palaikyti privatumo apsaugą, nes kiekvienas objektas prijungtas prie daiktų interneto sukelia dideles grėsmes saugumui, kurios susijusios su užfiksuotų slaptų duomenų apie jų savininkus arba vartotojus konfidencialumu, autentiškumu, duomenų ir paslaugų vientisumu;
- kokybiškos ir saugios paslaugos: daiktų internetas turi garantuoti aukštos kokybės ir didelio saugumo paslaugas, susijusias su žmogaus kūnu, nes jos remiasi paslaugomis teikiamomis fiksuojant, perduodant ir apdorojant duomenis, kurie parodo žmogaus statines savybes ir dinaminę elgseną;
- savaiminis diegimas: daiktų internetas turi turėti savaiminio diegimo technologiją, kuri įgalintų automatinę kartą arba semantika grindžiamą konfigūraciją, vientisam tarpusavyje susietų objektų sujungimui su programomis ir jų reikalavimais;
- valdymas: daiktų internetas turi nustatyti pavaldumą, siekiant užtikrinti patikimas tinklo operacijas, nes objektus valdančios programos paprastai

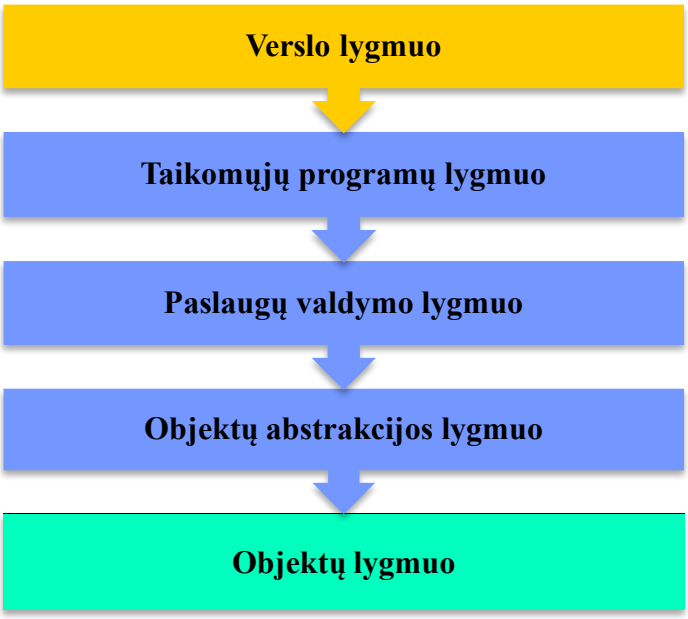
dirba automatiškai be tiesioginio žmonių dalyvavimo, tačiau jų visi veiklos procesai turi būti prižiūrimi ir kontroliuojami iš visiškai skirtingų vietų.

Viena iš svarbiausių daiktų interneto problemų yra laikoma daiktų interneto objektų identifikacija, kuri suteikia galimybę identifikuoti objektus ir nuskaityti jų informaciją be prisilietimo. Daiktų interneto objektų identifikacijos problema nėra nauja ir vienalytė, o greičiau tam tikras problemų mazgas, todėl jų sprendimui yra sukurta gausybė identifikavimo būdų ir nuolatos ieškoma naujų bei efektyvesnių (Madakam *et al.* 2015).

2. Daiktų interneto architektūra

Prie interneto prijungtų daiktų skaičius nuolat didėja ir prognozuojama, kad iki 2020-jų metų bus apie 50 milijardų sąveikomis susietų fizinių objektų. Toks daiktų interneto objektų mastas glaudžiai sujungia realų pasaulį su skaitmeniniu informacinių technologijų pasauliu, kuris grindžiamas automatinės identifikacijos, buvimo vietos realiame laike, jutiklių ir valdiklių technologijomis. Daiktų interneto pagalba turi būti galima susieti daugybę įvairių rūšių objektų per internetą, todėl reikalinga lanksti sluoksninė architektūra (Chen *et al.* 2014).

Iki šiol pasiūlytos daiktų interneto architektūros dar nėra tapusios etaloniniu modeliu, tačiau yra nuolat vystomi pasauliniai projektai mėginantys sukurti bendrąją architektūrą, remiantis įvairiomis mokslinėmis analizėmis ir pramonės poreikiais. Viena iš tokių pasiūlytų daiktų interneto architektūros modelių yra penkių sluoksnių architektūra 1 pav. susidedanti iš verslo, taikomųjų programų, paslaugų valdymo, objektų abstrakcijos ir objektų lygmenų (Wu *et al.* 2010; Khan *et al.* 2012).



1 pav. Daiktų interneto architektūra

Verslo lygmuo valdo daiktų interneto sistemos veiklą ir paslaugas. Jo pagrindinė atsakomybė yra kurti verslo modelius, diagramas, struktūrines schemas remiantis gautais duomenimis iš taikomųjų programų lygmens, o taip pat projektuoti, analizuoti, įgyvendinti, vertinti, stebėti ir kurti su daiktų interneto sistema susijusius elementus. Šis lygmuo leidžia palaikyti sprendimų priėmimo procesus, kurie yra grindžiami didžiųjų duomenų (angl. *Big Data*) analize, o taip pat stebėti ir valdyti žemiau esančius lygmenis. Verslo lygmuo išlygina kiekvieno sluoksnio išvestį su numatytu išėjimu tam, kad padidinti teikiamų paslaugų ir išlaikyti vartotojų privatumą (Muhic *et al.* 2014).

Taikomųjų programų lygmuo suteikia vartotojui tam tikras paslaugas (pvz., gali suteikti vartotojui reikiamus temperatūros ir oro drėgmės matavimus). Jis taip pat turi galimybę suteikti aukštos kokybės išmaniąsias paslaugas, siekiant patenkinti įvairius vartotojų poreikius. Šis lygmuo apima tokias rinkas kaip išmanieji namai, pastatai, medicina ir t. t. (Perera *et al.* 2013).

Paslaugų valdymo lygmuo arba tarpinės programinės įrangos lygmuo sujungia paslaugas su vartotoju remiantis adresais ir pavadinimais. Jis leidžia daiktų interneto taikomųjų programų programuotojui dirbti su įvairiais objektais be konkrečios techninės įrangos platformos. Šis sluoksnis apdoroja gautus duomenis, priima sprendimus ir pristato reikalingas paslaugas per tinklo protokolus (Liu *et al.* 2012).

Objektų abstrakcijos lygmuo perduoda objektų lygmenyje sukurtus duomenis į paslaugų valdymo lygmenį per saugius kanalus. Šis lygmuo suderina prieigą prie įvairių objektų duomenų naudodamas bendrą kalbą ir procedūras. Duomenys gali būti

perduodami per tokias technologijas kaip RFID, 3G, GSM, UMTS, WiFi, Bluetooth, IR, ZigBee ir kt. Šiame lygmenyje tvarkomi duomenų valdymo procesai, debesų skaičiavimai ir kitos funkcijos (Mitton *et al.* 2011; Hemalatha *et al.* 2015).

Objektų lygmuo parodo daiktų interneto fizinius jutiklius, kuriais surenkama ir apdorojama informacija. Jis apima jutiklius ir valdiklius tam, kad atlikti įvairias užklausas apie būseną, drėgmę, slėgį, svorį, vietą ir pan. Standartiškai savaiminio diegimo mechanizmams yra reikalingas sąvokos lygmuo tam, kad sukonfigūruoti įvairius objektus. Sąvokos lygmuo skaitmenizuoja ir persiunčia duomenis į objekto abstrakcijos lygmenį per saugius kanalus. Šiame lygmenyje yra priimami daiktų interneto didieji duomenys (Kuyoro *et al.* 2015).

3. Daiktų interneto elementai

Daiktų interneto elementai 2 pav. padeda geriau suprasti tikrąją daiktų interneto reikšmę ir funkcionalumą, kurį užtikrina identifikavimas, fiksavimas, komunikacija, skaičiavimai, paslaugos ir semantika (Shah *et al.* 2016).

2 pav. Daiktų interneto elementai:
a) identifikavimas, b) fiksavimas, c) komunikacija, d) skaičiavimai, e) paslaugos, f) semantika

Identifikavimas yra svarbus daiktų internete, norint pavadinti ir suderinti paslaugas su jų užklausomis. Adresuojant daiktų interneto objektus reikia diferencijuoti tarp objekto identifikatoriaus ir jo adreso. Objekto identifikatorius nurodo savo vardą jutikliui ir jo adresas per komunikacijos tinklą perduodamas į nurodytą vietą. Skirtumas tarp objektų identifikavimo ir adresavimo yra būtinas, nes identifikavimo būdai nėra visur vienodi. Identifikavimas yra naudojamas siekiant suteikti objektams tinkle aiškią tapatybę (Choudhary *et al.* 2016).

Fiksavimas daiktų internete reiškia duomenų rinkimą iš tarpusavyje susietų objektų tinkle ir jų siuntimą atgal į duomenų saugyklą, duomenų bazę arba debesį. Surinkti duomenys yra analizuojami norint atlikti veiksmus, kurie yra grindžiami reikalingomis paslaugomis. Daiktų interneto jutikliai gali būti išmanūs priėmimo elementai, valdikliai arba nešiojami fiksavimo įrenginiai (Mačiulienė *et al.* 2012).

Komunikacija daiktų internete jungia tarpusavyje įvairius objektus tam, kad būtų galima teikti konkrečias išmaniąsias paslaugas. Dažniausiai daiktų interneto mazgai turi veikti naudodami mažai energijos esant komunikacijos ryšiams su galimais praradimais ir triukšmais (Miettinen *et al.* 2017).

Skaičiavimai daiktų internete atliekami dėka mikrovaldiklių ir taikomosios programinės įrangos, kuri simbolizuoja „protingus smegenis“ ir skaičiavimo galimybes. Daugelis programinės įrangos platformų yra naudojamos teikti daiktų interneto funkcijas, kur tarp jų operacinės sistemos yra labai svarbios, nes veikia visą įrenginio aktyvacijos laiką. Debesų platformos taip pat sudaro kitą svarbią daiktų interneto skaičiavimų dalį. Jos suteikia sąlygas išmaniesiems objektams siųsti savo duomenis į debesis, didiesiems duomenims būti tvarkomiems realiu laiku, o tiesioginiams vartotojams gauti naudos iš žinių, kurios buvo išgautos iš didžiųjų duomenų (Granjal *et al.* 2015).

Paslaugos daiktų internete skirstomos į tapatybės nustatymo, informacijos surinkimo, bendrąsias ir universaliąsias paslaugas. Tapatybės nustatymo paslaugos yra pagrindinės ir svarbiausios, nes kiekviena programa turi perkelti realaus pasaulio objektus į informacijos pasaulį ir juos identifikuoti. Informacijos surinkimo paslaugos surenka ir apibendrina pradinius sensoriaus matavimus, kurie turi būti apdoroti ir perduoti į daiktų interneto programas. Bendrosios paslaugos veikia informacijos surinkimo paslaugų viršuje, naudoja išgautus duomenis priimant sprendimus ir atitinkamai reaguoja. Universaliosios paslaugos suteikia bet kuriuo metu bendrąsias paslaugas, kai tik jos yra kam nors reikalingos. Pagrindinis daiktų interneto programų tikslas yra pasiekti universalių paslaugų lygį, tačiau tai nėra lengva, nes yra dar daug problemų, kurios turi būti ateityje išspręstos (Jia *et al.* 2012).

Semantika daiktų internete reiškia visapusišką gebėjimą išmaniai išgauti žinias iš skirtingų mechanizmų tam, kad suteikti reikalingas paslaugas. Žinių gavyba apima išaiškinimą, resursų naudojimą, modeliavimo informaciją, duomenų atpažinimą ir informacijos analizavimą, norint suprasti teisingo sprendimo prasmę suteikiant tikslias

paslaugas. Tokiu būdu semantika vaizduoja daiktų interneto intelektą, siunčiant poreikius į reikiamą resursą (Gazis *et al.* 2015).

4. Daiktų interneto objektų identifikavimo protokolai

Šiuo metu egzistuoja visa aibė standartizuotų technologijų, kurios yra plačiai paplitusios, gerai ištirtos ir įvertintos įvairių kriterijų požiūriu, todėl jas suskirstysime pagal daiktų interneto elementus ir pateiksime 1 lentelėje (Al-Fuqaha *et al.* 2015).

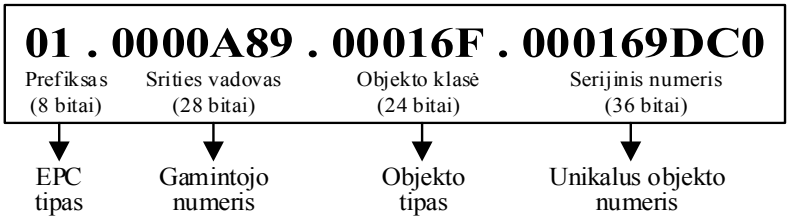
Elektroninis produkto kodas (angl. *Electronic Product Code* – EPC) yra unikalus identifikavimo numeris, kuris skirtas identifikuoti fizinius objektus. EPC ne tik leidžia identifikuoti objektus, bet ir gauti informaciją apie juos per informacijos paslaugų sistemą. Naudojant EPC identifikuotiems objektams priskiriami unikalūs serijos numeriai, todėl kiekvieno objekto EPC yra skirtingas. Toks būdas leidžia unikaliai, tiksliai ir konkrečiai identifikuoti atskirus objektus (An *et al.* 2012).

1 lentelė. Daiktų interneto elementų technologijos

Daiktų interneto elementai		**Technologijos**
Identifikavimas	Vardas	EPC, uCode
	Adresas	IPv4, IPv6
Fiksavimas		Išmanūs jutikliai, montuojami jutikliai, nešiojami jutikliai, valdikliai, etiketės
Komunikacija		RFID, NFC, UWB, Bluetooth, Z-Wave, BLE, IEEE 802.15.4, BLE, LTE-A, WiFi, WiFiDirect
Skaičiavimai	Aparatūra	SmartThings, Intel Galileo, Cubieboard Arduino, Gadgeteer, Phidgets, Raspberry Pi, BeagleBone
	Programos	Contiki, TinyOS, LiteOS, Riot OS, Android, Nimbits, Hadoop
Paslaugos		Tapatybės nustatymo, informacijos surinkimo, bendrosios, universalios
Semantika		RDF, OWL, EXI

EPC struktūrą 3 pav. sudaro 64 bitų arba 96 bitų ilgio informacija, kurioje yra EPC tipas, gamintojo numeris, objekto tipas ir unikalus objekto numeris. EPC 64 bitų kodas palaiko apie 16 tūkstančių gamintojų su skirtingais numeriais, apima nuo 1 iki 9 milijonų įvairių objektų tipų ir saugo 33 milijonus unikalių serijos numerių kiekvienam objekto tipui. EPC 96 bitų kodas palaiko apie 268 milijonus gamintojų su skirtingais numeriais, apima nuo 16 milijonų įvairių objektų tipų ir saugo 68 milijardus unikalių

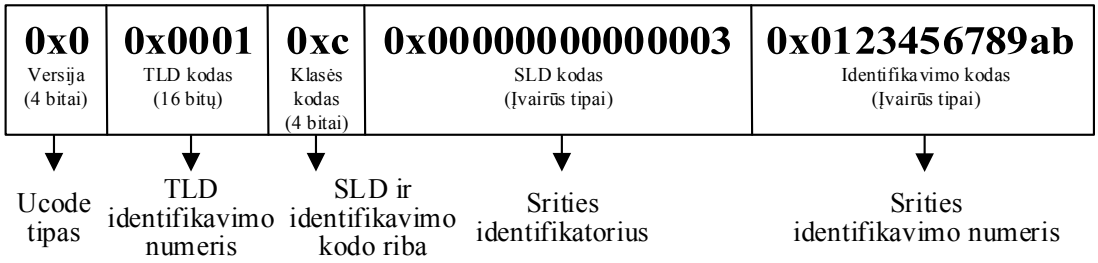
serijos numerių kiekvienam objekto tipui (Miorandi *et al.* 2012; Guo *et al.* 2013).



3 pav. EPC struktūra

Ucode yra unikalus identifikavimo numeris, kuris skirtas identifikuoti objektus, vietas ir konceptus realiame pasaulyje. Pats Ucode nesusietas su identifikuojamu resursu ir sugeneruojamas visiškai nepriklausomai. Jo priskyrimu rūpinasi aukščiausio lygio srities (angl. *Top Level Domain* – TLD) ir antro lygio srities (angl. *Second Level Domain* – SLD) organizacijos, o klientai norėdami prieiti prie resurso, kreipiasi į duomenų bazę, kuri pagal kodą grąžina nuorodą į resursą. uCode tinka identifikuoti, bet kokio tipo resursus ir visiškai nepriklauso nuo taikymo srities (Gigli *et al.* 2011).

Ucode struktūrą 4 pav. sudaro 128, 256 ar 512 bitų ilgio informacija, kurioje yra versija, TLD kodas, klasės kodas, SLD kodas ir identifikavimo kodas. Versija nurodo Ucode tipą, kuris yra žymimas dvejetainiu skaičiumi. TLD kodas apibrėžia rezervuotą vietą, kuri skirta unikalių identifikatorių žymoms ir Ucode numeriams. Klasės kodas nusako ribą tarp SLD ir identifikavimo kodo. SLD kodas yra apibūdinamas kaip žemesnio lygio Ucode vietos domenas ir identifikuoja kiekvieną sritį. Identifikavimo kodas nustato individualų tapatybės nustatymo numerį (Lee *et al.* 2011).

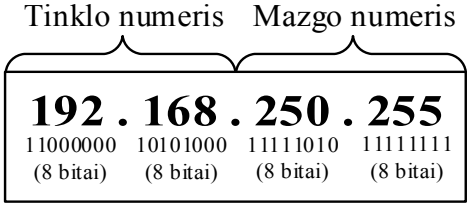


4 pav. Ucode struktūra

Interneto protokolas (angl. *Internet Protocol* – IP) yra taisyklių rinkinys, reglamentuojantis daiktų interneto objektų adresavimą, duomenų skaidymą į mažesnius paketus prieš siunčiant ir surinkimą juos atsiuntus, o taip pat jų tolimesnių maršrutų parinkimą. IP kartu su perdavimo valdymo protokolu (angl. *Transmission Control*

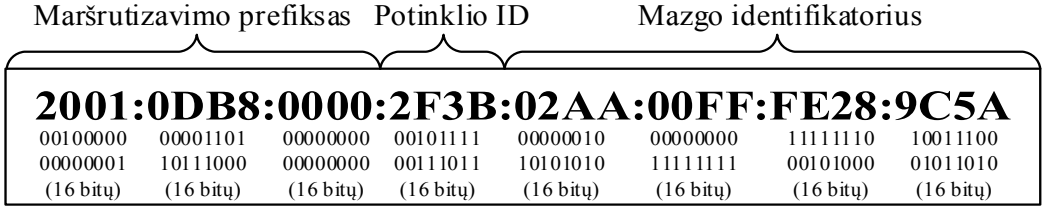
Protocol – TCP) sudaro TCP/IP protokolą, kuris yra pagrindinis interneto protokolas. Taip pat jis yra TCP/IP rinkinio protokolas adresuojantis ir maršrutizuojantis duomenis, kuris atsako už vieno duomenų paketo gabenimą iš mazgo į kitą mazgą. IP tiksliai apibrėžia, kad kiekvienas objektas turi unikalų numerį, kuris yra vadinamas interneto protokolo adresu (angl. *Internet Protocol Address*). Šiuo metu plačiausiai yra paplitusi ketvirtoji protokolo versija IPv4, tačiau naujausia šeštoji protokolo versija IPv6 ją palaipsniui keičia (Atzori *et al.* 2010).

IPv4 naudoja 32 bitus adresui užrašyti, o tai apima apie 2^{32} įvairių interneto objektų. Jis buvo sukurtas taip, kad turėtų minimalią perteklinę informaciją, nepriklausytų nuo kanalinio ir fizinio lygmens technologijų, o prieš paketų siuntimą būtų neatliekama papildomų sujungimo veiksmų ir nenaudojama papildoma informacija patikimumui užtikrinti. IPv4 struktūrą 5 pav. sudaro 4 dešimtainiai skaičiai nuo 0 iki 255, kurie tarpusavyje atskirti taškais. IPv4 adresą sudaro tinklo numeris ir mazgo šiame tinkle numeris. Tinklo numeris skirtas tinklui pažymėti ir naudojamas maršrutizuojant paketus. Mazgo numeris yra priskiriamas konkrečiam tinklo objektui (Salman *et al.* 2014).



5 pav. IPv4 struktūra

IPv6 naudoja 128 bitus adresui užrašyti, o tai apima apie 2^{128} įvairių interneto objektų. IPv6 struktūrą 6 pav. sudaro 8 šešioliktainiai skaičiai, kurie tarpusavyje atskirti dvitaškiais. IPv6 struktūroje viena nuo kitos yra išskiriama tinklo ir mazgo dalis, kur 64 bitai naudojami tinklo daliai ir maršrutizavimui, o likusieji 64 bitai skirti mazgo identifikavimui (Jara *et al.* 2012).



6 pav. IPv6 struktūra

5. Daiktų interneto objektų identifikavimo standartai

Daugelis daiktų interneto objektų identifikavimo standartų yra sukurti siekiant palengvinti taikomųjų programų programuotojų ir įvairias paslaugas teikiančių organizacijų darbus. Šie standartai tarpusavyje skiriasi duomenų sparta, veikimo nuotoliu, energijos sąnaudomis, saugumo lygiu, naudojamų dažnių ir kt. parametrais. Skirtingos tarptautinių standartų kūrimo organizacijos palaiko daiktų interneto objektų identifikaciją kaip pasaulinis žiniatinklio konsorciumas (angl. *World Wide Web Consortium* – W3C), interneto inžinerijos darbo grupė (angl. *Internet Engineering Task Force* – IETF), elektroninių produktų kodų įmonė (angl. *Electronic Product Code Company* – EPCglobal), elektrotechnikos ir elektronikos inžinierių institutas (angl. *Institute of Electrical and Electronics Engineers* – IEEE) ir Europos telekomunikacijų standartizacijos institutas (angl. *European Telecommunications Standards Institute* – ETSI). Šių tarptautinių organizacijų sukurti daiktų interneto standartai yra suklasifikuoti į atskiras programų, paslaugų teikimo, infrastruktūros, įtakos grupes ir pateikti 2 lentelėje (Bandyopadhyay *et al.* 2011).

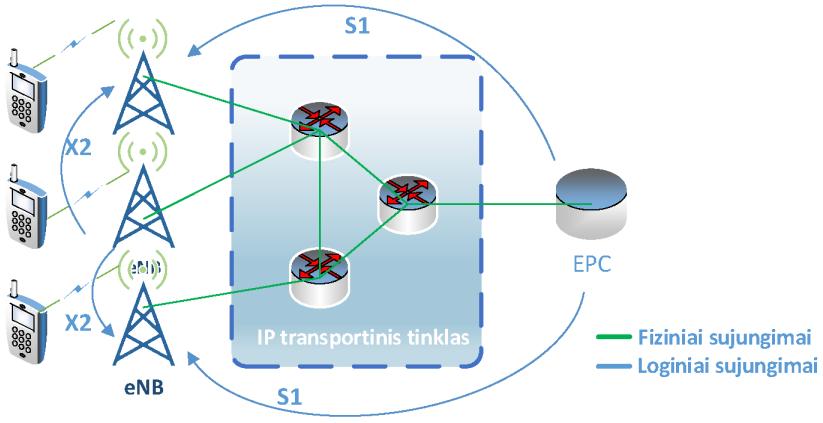
2 lentelė. Daiktų interneto standartai

<table>
<tr><th colspan="2">Programų standartai</th><th>DDS</th><th>CoAP</th><th>AMQP</th><th>MQTT</th><th>MQTT-SN</th><th>XMPP</th><th>HTTP REST</th></tr>
<tr><td colspan="2">Paslaugų teikimo standartai</td><td colspan="4">mDNS</td><td colspan="3">DNS-SD</td></tr>
<tr><td rowspan="4">Infrastruktūros standartai</td><td>Maršruto lygmuo</td><td colspan="7">RPL</td></tr>
<tr><td>Tinklo lygmuo</td><td colspan="5">6LoWPAN</td><td colspan="2">IPv4/IPv6</td></tr>
<tr><td>Ryšio lygmuo</td><td colspan="7">ZigBee</td></tr>
<tr><td>Objektų lygmuo</td><td>LTE-A</td><td colspan="2">EPCglobal</td><td colspan="2">IEEE 802.15.4</td><td colspan="2">Z-Wave</td></tr>
<tr><td colspan="2">Įtakos standartai</td><td colspan="2">IEEE 1888.3</td><td colspan="2">IPSec</td><td colspan="3">IEEE 1905.1</td></tr>
</table>

Mobiliojo ryšio standartas LTE-A (angl. *Long Term Evolution-Advanced* – LTE-A) apima daugumą tinklo komunikacijos protokolų, kurie tinka mašinų grupės komunikavimui (angl. *Machine Type Communications* – MTC), daiktų interneto infrastruktūrai ir išmaniesiems miestams. Objektų lygmenyje LTE-A standartas naudoja ortogonalų dažnių dalijimąsi daugialype prieiga (angl. *Orthogonal Frequency Division*

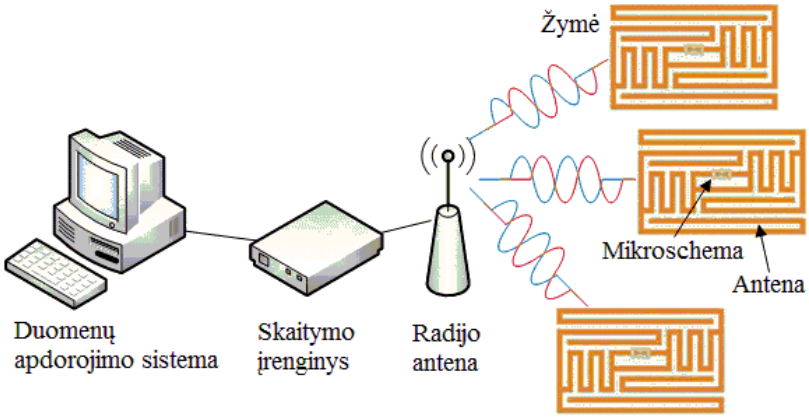
Multiple Access – OFDMA), kuria kanalo dažnių juostos plotis yra padalijamas į mažesnes juostas. Taip pat LTE-A standartas naudoja daugelio sudedamųjų nešlių (angl. *Component Carrier* – CC) skleidimo spektrų techniką, kuri leidžia turėti iki 5 nešančiųjų dažnių su 20 MHz dažnių juostos pločiu. Tokios perdavimo spartos turėtų būti pasiektos išlaikant esamą LTE standarto radijo dažnio spektrą be neigiamo poveikio vartotojų įrenginiams (Kocakulak *et al.* 2017).

LTE-A tinklas 7 pav. sudarytas iš dviejų pagrindinių sudedamųjų dalių. Pirmoji sudedamoji dalis yra pagrindinis tinklas (angl. *Core Network* – CN), kuris kontroliuoja mobiliuosius įrenginius ir susijęs su IP paketų srautais. Antroji sudedamoji dalis yra radijo prieigos tinklas (angl. *Radio Access Network* – RAN), kuris reguliuoja bevielio ryšio, radijo prieigos, vartotojo ir valdymo plokštumų protokolus. RAN susideda iš radijo valdymo įrangos (angl. *Integrated Network Controller* – INC), mažų ekonomiškų galinių tinklo įrenginių ir atsparių išorinėms lauko sąlygoms bazinių stočių, kurios yra sujungtos X2 sąsajomis. RAN ir CN yra sujungtos S1 sąsajomis. Mobilūs arba MTC įrenginiai gali prisijungti prie bazinių stočių tiesiogiai arba per MTC vartus. Jie taip pat turi tiesioginį ryšį su kitais MTC įrenginiais (Palattella *et al.* 2016).



7 pav. LTE-A tinklo struktūra

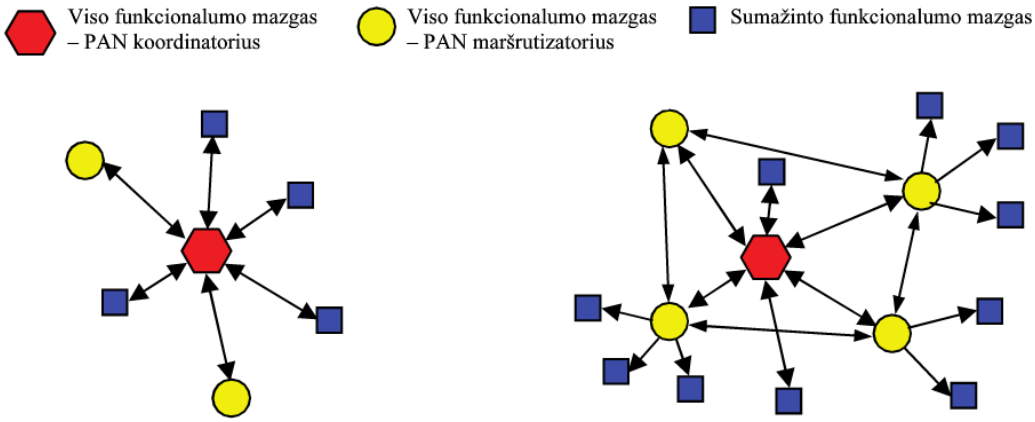
EPCglobal standartas aprašo EPC naudojimą žymėse ir brūkšniniuose koduose, kurie talpina įvairią informaciją apie nutolusius objektus. EPCglobal sistemą 8 pav. sudaro duomenų apdorojimo sistema, skaitymo įrenginys, radijo antena, žymė su įmontuota mikroschema ir nedidele antena, kurią galima pritvirtinti prie objekto, o informaciją nuskaityti radijo dažnio atpažinimo aparatūra. Nuotolinis žymės identifikavimas suteikia plačias sistemos pritaikymo galimybes gamybos, logistikos, prekybos ir kitose įmonėse (Pardal *et al.* 2010).



8 pav. EPCglobal sistemos struktūra

IEEE 802.15.4 standartas skirtas belaidžių jutiklių tinklams (angl. *Wireless Sensor Network* – WSN) sujungti, kurie yra nedidelių funkcinių galimybių. Dėl šio standarto charakteristikų, tokių kaip mažos energijos sąnaudos, nedidelė duomenų perdavimo sparta, aukštas pranešimų pralaidumas yra naudojamas IoT, M2M ir WSN. Jis suteikia patikimą ryšį, veiksmingumą tarp skirtingų platformų, valdomumą esant dideliam skaičiui mazgų, aukštą saugumo lygį, šifravimo ir autentifikavimo paslaugas. IEEE 802.15.4 standartas palaiko skirtingų dažnių kanalų juostas ir naudoja tiesinės sekos spektro sklaidos (angl. *Direct Sequence Spread Spectrum* – DSSS) technologiją. Naudojamų dažnių kanalais objektų lygmuo perduoda ir priima duomenis per tris dažnių juostas: 250 kbps prie 2,4 GHz, 40 kbps prie 915 GHz ir 20 kbps prie 868 GHz. Aukštesni dažniai suteikia didelį pralaidumą ir mažą uždelsimą, o žemesni dažniai suteikia geresnį jautrumą ir padengia didelius atstumus (Roman *et al.* 2011).

IEEE 802.15.4 standartas palaiko viso funkcionalumo (angl. *Full Function Device* – FFD) ir sumažinto funkcionalumo (angl. *Reduced Function Device* – RFD) tinklo mazgus. RFD mazgas paprastai priima ir siunčia jutiklio duomenis. FFD mazgai gali būti asmeninės erdvės tinklo (angl. *Personal Area Network* – PAN) koordinatoriais, maršrutizatoriais arba paprastais mazgais. PAN tinklo koordinatorius yra pagrindinis tinklo mazgas, kuris kuria tinklą, priima į jį kitus mazgus ir sinchronizuoja jų veikimą. IEEE 802.15.4 standartas 9 pav. numato žvaigždinę (angl. *Star*) ir iš mazgo į mazgą (angl. *Peer-Peer*) tinklo topologijas. Žvaigždinės topologijos tinkle mazgai komunikuoja tiesiogiai su koordinatoriumi, todėl jame nenaudojami maršrutizatoriai. Topologijos iš mazgo į mazgą tinkle naudojami maršrutizatoriai, kurie yra komunikavimo tarpininkai, galintys persiųsti mazgų pranešimus (Li *et al.* 2015).



a) b)

9 pav. IEEE 802.15.4 tinklo topologijos:
a) žvaigždinė, b) iš mazgo į mazgą

Mažos galios belaidžio ryšio komunikacijos Z-Wave standartas yra skirtas namų automatizacijos tinklams (angl. *Home Automation Networks* – HAN) ir nuotoliniam objektų valdymui. Šis standartas yra naudojamas žemo duomenų perdavimo reikalaujančiose vietose, kuriose veikia mažą energijos kiekį vartojantys radijo siųstuvai ir imtuvai. Z-Wave tinklas 10 pav. veikia 900 MHz dažnio juostose ir suteikia 40 kbps duomenų perdavimo greitį (Tan *et al.* 2014).

10 pav. Z-Wave tinklo struktūra

6. Daiktų interneto objektų identifikavimo metodai

Daiktų internete objektai yra pasiskirstę supančioje aplinkoje, todėl būtina turėti tam tikrą mechanizmą, kuris leistų identifikuoti ir atrasti vienas nuo kito nutolusius įvairius daiktų interneto įrenginius. Daiktų interneto objektų identifikavimo metodai

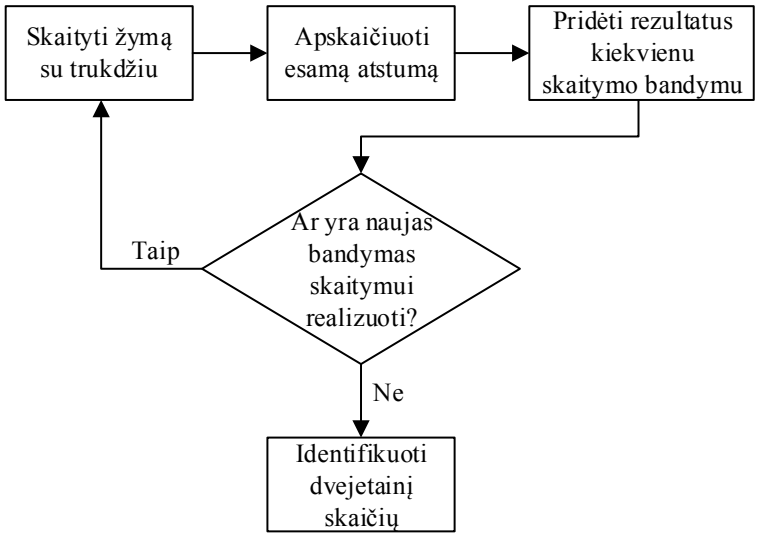
leidžia vartotojams interaktyviai sąveikauti su asmeniniais daiktais turinčiais identifikatorius ir gauti įvairiausias šiuolaikines paslaugas. Prie tokių yra priskiriami radijo dažnio identifikavimo (angl. *Radio Frequency Identification* – RFID), bendro resursų identifikavimo (angl. *Uniform Resource Identification* – URI) ir skaitmeninio objekto identifikavimo (angl. *Digital Object Identification* – DOI) daiktų interneto metodai (Sun *et al.* 2015; Meidan *et al.* 2017).

RFID metodas yra naudojamas daiktų interneto objektams identifikuoti ir sekti. Jį sudaro dvejetainio kodo skaitymo bandymų skaičius, fiksuotų bandymų dvejetainis kodas, dvejetainis žymos kodas, kuris yra saugojamas duomenų bazėje. RFID metodas nuskaito duomenis saugomus objekto žymoje naudodamas tris pagrindinius dažnių diapazonus (Kim *et al.* 2014):

- 13,56 MHz aukšto dažnio diapazonas (angl. *High Frequency* – HF), pasižymintis trumpu žymės duomenų nuskaitymo atstumu;
- 860 – 960 MHz ultra aukšto dažnio diapazonas (angl. *Ultra High Frequency* – UHF), galintis nuskaityti žymės duomenis vidutiniu atstumu;
- 2,45 GHz super aukšto dažnio diapazonas (angl. *Super High Frequency* – SHF), išsiskiriantis dideliu žymės duomenų nuskaitymo atstumu.

RFID metodas 11 pav. prasideda nuo žymos su trukdžiu skaitymo. Nuskaičius tokią žymą yra gaunamas dvejetainis kodas, kuris gali būti neteisingas dėl aplinkos trukdžių. Gauto su trukdžiais dvejetainio kodo atstumo skirtumas, apskaičiuojamas atsižvelgiant į žymos kodą. Kiekvienu žymos skaitymo bandymu, gautas atstumo skirtumas yra pridedamas. Sprendimas atlikti didesnį skaičių bandymų yra ankstesnės duomenų apdorojimo posistemės konfigūracijos rezultatas (Escobar *et al.* 2015):

1. Realizuoti fiksuotą skaičių bandymų tam, kad būtų galima identifikuoti objekto žymą didelių trukdžių aplinkoje, kur skaitymų bandymų skaičius nėra optimizuotas konkrečiai aplinkai.
2. Realizuoti fiksuotą skaičių bandymų grindžiamų trukdžių specifinėje aplinkoje tipu ir lygiu, kur objekto žyma bus nuskaitoma.
3. Dinamiškai nustatyti bandymų skaičių grindžiamų apskaičiuotais skirtumų atstumais, kur bandymai pasibaigia kai skirtumas tarp minimalios sumos ir likusių sumų pasiekia iš anksto numatytą toleranciją.



11 pav. RFID metodas

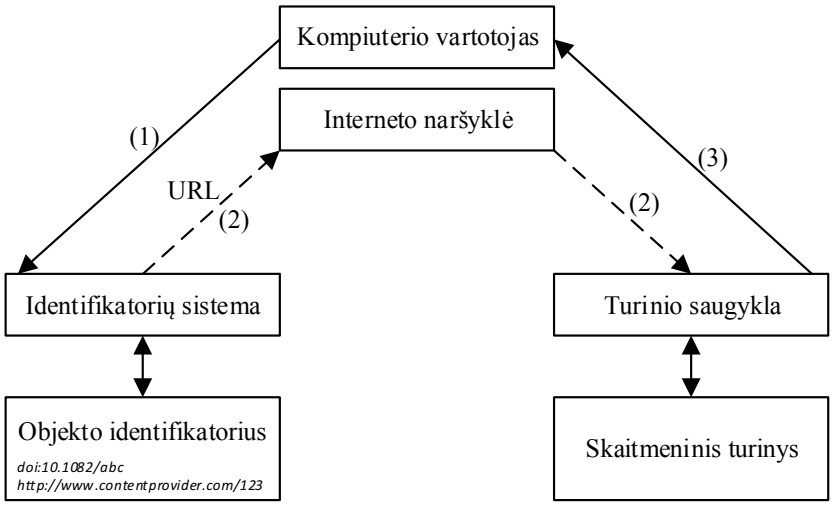
URI metodas yra naudojamas fizinių arba informacijos daiktų interneto objektų identifikavimui. Jį sudaro simbolių seka iš amerikietiškos informacijos mainų koduotės standarto. URI metodas susideda iš daiktų interneto simbolių ir tęsiamas po dvitaškio. Du pasviri brūkšniai nurodo kelią, kuris yra koduojamo objekto loginis adresas. Kelio seka yra atskiriama pasvirais brūkšniais ir toliau aprašomos fizinių objektų erdvinės vietos. Sąsaja yra išskirta nuo ankstesnės dalies grotažyme bei atsakinga už jutiklių su internetu sujungimą. Objekto identifikacinis numeris nurodo fizinio objekto vardą ir gali būti sudarytas iš įvairių raidžių, kurių derinys turi būti unikalus (Ma *et al.* 2015).

URI metodas 12 pav. charakterizuoja tinkle esančius fizinius objektus pagal medžio hierarchiją. Aikštė nurodo medžio šakninį mazgą, toliau esantis lygmuo reiškia pastatą, o visi kiti likę lygmenys žymi pastato grindis ir kambarius. Pirmame kambaryje įrengtas dūmų jutiklis, antrame kambaryje sumontuotas drėgmės jutiklis, o trečiame kambaryje įtaisytas vandens jutiklis yra prijungtas prie tinklo (Wen *et al.* 2016).

DOI metodas yra naudojamas daiktų interneto objektams identifikuoti skaitmeninėje erdvėje. Jį sudaro simbolių seka iš priešdėlio ir priesagos, kurie tarpusavyje yra atskirti pasvirusiu brūkšniu. Priešdėlis yra katalogo ir registravimo kodų tarpusavio derinys, kuris nurodo identifikuojamo daiktų interneto objekto savininką. Priesaga sudaryta iš identifikatoriaus simbolių sekos ir nustato daiktų interneto objekto informaciją, kuri priešdėliui yra visada skirtinga. Priešdėlio ir priesagos kombinacija neturi simbolių sekos ilgiui apribojimų, o taip pat ir kitoms sudedamosioms dalims, kurios yra visuotinai unikalios (Park *et al.* 2011).

DOI metodas 13 pav. susideda iš trijų etapų, kuriuos įvykdžius yra gaunami

objekto identifikavimo rezultatai. Pirmame etape kompiuterio vartotojas per interneto naršyklę siunčia užklausą identifikatorius saugančiai sistemai. Ši sistema patikimai saugo nuolatinius objektų identifikatorius su jungtiniais duomenimis, kuriuos galima automatiškai pakeisti į bendrus resursų adresus (angl. *Uniform Resource Locator* – URL) su papildomais metaduomenimis. Antrame etape grąžinamas atsakymas į pateiktą kompiuterio vartotojo užklausą su tiksliais objekto identifikavimo duomenimis. Trečiame etape interneto naršyklei su identifikatorių sistemos pateiktais duomenis arba URL suteikiama prieiga prie informacijos, kurią atsiunčia turinio saugykla pagal kompiuterio vartotojo užklausą (Danilov *et al.* 2016).



13 pav. DOI metodas

Atliekant daiktų interneto identifikavimo metodų palyginimą yra naudojama stiprybių, silpnybių, galimybių, grėsmių (angl. *Strengths, Weaknesses, Opportunities, Threats* – SWOT) analizė, kurios rezultatai pateikti 3 lentelėje.

3 lentelė. RFID, URI, DOI metodų palyginimas

Metodo savybės	RFID metodas	URI metodas	DOI metodas
Stiprybė	Centralizuotas	Paprastas	Tikslus
Silpnybė	Nestandartizuotas	Išplėstas	Nederantis
Galimybė	Prisitaikantis	Trumpinamas	Plečiamas
Grėsmė	Neuniversalus	Nesaugus	Nepatikimas

7. Išvados

1. Daiktų internetas yra neatskiriama ateities interneto dalis, kuri apibrėžiama kaip pasaulinė ir dinaminė tinklo infrastruktūra, grindžiama standartiniais ir suderinamais komunikacijos protokolais, kur fiziniai ir informacijos objektai turi identifikacines savybes, fizinius atributus, informacines personalijas, naudoja išmaniąsias sąsajas ir tiesiogiai komunikuoja su kitais objektais.
2. Daiktų interneto architektūra turi turėti lanksčias sąsajas, kurios užtikrintų paskirstyto tipo daiktų interneto resursų tarpusavio sąveiką, saugumą ir patikimumą, palaikytų universalius daiktų interneto objektų identifikacijos protokolus ir standartus.
3. Daiktų internetas apibrėžia išmanią aplinką, kurioje fiziniai daiktai įgauna tarpusavio komunikavimo galimybes ir tiesiogiai įjungti į vientisą informacinį tinklą, kuriame daiktai tampa aktyvūs verslo procesų dalyviai, todėl siekiant, kad daiktų interneto objektai galėtų tarpusavyje komunikuoti yra reikalingas daiktų interneto objektų identifikavimo metodas.
4. Daiktų interneto identifikacijos protokolų ir standartų apžvalga parodė, kad šias technologijas galima suskirstyti į identifikacijos technologijas, naudojančias centrinę duomenų bazę identifikuojamų objektų metaduomenims saugoti ir paskirstytas identifikacijos sistemas, kuriose informacija apie daiktų interneto objektų paslaugas ir resursus yra paskirstyta daiktų interneto mazguose.
5. Daiktų interneto objektų identifikavimo metodų apžvalga ir palyginimas parodė, kad prieigos kontrolės panaudojimas leidžia apsaugoti daiktų interneto objektų duomenis nuo nesankcionuoto naudojimo ir leidžia informaciją pasiekti tik įgaliotiems vartotojams.

8. Literatūra

1. AL-FUQAHA, A.; GUIZANI, M.; MOHAMMADI, M.; ALEDHARI, M. (2015). IoT: A Survey on Enabling Technologies, Protocols, and Applications, *Journal of IEEE Communications Surveys and Tutorials* 17(4): 2347–2376.
2. AN, J.; GUI, X. L.; HE, X. (2012). Study on the Architecture and Key Technologies for Internet of Things, in *Proc. of the 7th Conference on Electrical and Computer*

Engineering (ICECE), December 20–22, 2012, Dhaka, Bangladesh, 329–335.

3. ATZORI, L.; IERA, A.; MORABITO, G. (2010). The Internet of Things: A Survey, *Journal of Computer and Telecommunications Networking* 54(15): 2787–2805.
4. BANDYOPADHYAY, D.; SEN, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization, *International Journal of Wireless Personal Communications* 58(1): 49–69.
5. CHEN, S.; XU, H.; LIU, D.; WANG, H. (2014). A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective, *International Journal of IEEE Internet of Things* 1(4): 349–359.
6. CHOUDHARY, G.; JAIN, A. K. (2016). Internet of Things: A Survey on Architecture, Technologies, Protocols and Challenges, in *Proc. of the 2nd International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, December 23–25, 2016, Jaipur, India, 1–8.
7. DANILOV, K. N.; KULIK, V. A.; KIRICHEK, R. V. (2016). Review and Analysis of Methods of Identification and Authentication of the Internet of Things, *Journal of Information Technology and Telecommunications* 1(3): 49–57.
8. ESCOBAR, L. H.; SMITH, N. R.; CRUZ, J. R. R.; BARRON, L. E. C. (2015). Methods of Selection and Identification of RFID Tags, *International Journal of Machine Learning and Cybernetics* 6(5): 847–857.
9. ESPADA, J. P.; MARTINEZ, O. S.; BUSTELO C. P. G.; LOVELLE, J. M. C. (2011). Virtual Objects on the Internet of Things, *International Journal of Interactive Multimedia and Artificial Intelligence* 1(4): 24–30.
10. GAZIS, V.; GORTZ, M.; HUBER, M.; LEONARDI, A.; MATHIOUDAKIS, K.; WIESMAIER, A.; ZEIGER, F.; VASILOMANOLAKIS, E. (2015). A Survey of Technologies for the Internet of Things, in *Proc. of the 11th International Conference on Wireless Communications and Mobile Computing (IWCMC),* August 24–28, 2015, Dubrovnik, Croatia, 1090–1095.
11. GIGLI, M.; KOO, S. (2011). Internet of Things: Services and Applications Categorization, *Journal of Advances in Internet of Things* 1(2): 27–31.
12. GRANJAL, J.; MONTEIRO, E.; SILVA, J. S.; (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, *International Journal of IEEE Communications Surveys and Tutorials* 17(3): 1294–1312.
13. GUBBI, J.; BUYYA, R.; MARUSIC, S.; PALANISWAMI, M. (2013). Internet of

Things (IoT): A Vision, Architectural Elements, and Future Directions, *Journal of Future Generation Computer Systems* 29(7): 1645–1660.

14. GUO, Z. J. (2013). Research on Key Technologies and Application of Internet of Things, in *Proc. of the 25th Chinese Control and Decision Conference (CCDC)*, May 25–27, 2013, Guiyang, China, 2797–2801.
15. HEMALATHA, D.; AFREEN, B. E. (2015). Development in Radio Frequency Identification Technology in Internet of Things, *International Journal of Advanced Research in Computer Engineering and Technology* 4(11): 4030–4038.
16. JARA, A. J.; ZAMORA, M. A.; SKARMETA, A.; (2012). Glowbal IP: An Adaptive and Transparent IPv6 Integration in the Internet of Things, *International Journal of Mobile Information Systems* 8(3): 177–197.
17. JIA, X.; FENG, Q.; FAN, T.; LEI, Q. (2012). RFID Technology and its Applications in Internet of Things (IoT), in *Proc. of the 2th Conference on Consumer Electronics, Communications and Networks*, April 21–23, 2012, Yichang, China, 1282–1285.
18. KHAN, R.; KHAN, S. U.; ZAHEER, R.; KHAN, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, in *Proc. of the 10th Conference on Frontiers of Information Technology (FIT)*, December 17–19, 2012, Islamabad, Pakistan, 257–260.
19. KIM, K. J.; HONG, S. P. (2014). A Study on the Development Method for Trust-Based Activation in Internet of Things, *International Journal of Contemporary Engineering Sciences* 7(31): 1715–1721.
20. KOCAKULAK, M.; BUTUN, I. (2017). An Overview of Wireless Sensor Networks Towards Internet of Things, in *Proc. of the 7th Computing and Communication Workshop and Conference,* January 9–11, 2017, Las Vegas, Nevada, USA, 1–6.
21. KRAIJAK, S.; TUWANUT, P. (2015). A Survey on Internet of Things Architecture, Protocols, Possible Applications, Security, Privacy, Real-World Implementation and Future Trends, in *Proc. of the 16th International Conference on Communication Technology,* October 18–20, 2015, Hangzhou, China, 28–31.
22. KUYORO, S.; OSISANWO, F.; AKINSOWON, O. (2015). Internet of Things (IoT): An Overview, in *Proc. of the 3th International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM),* March 23–24, 2015,

London, United Kingdom, 53–58.

23. LEE, G. M.; CRESPI, N. (2011). Internet of Things for Smart Objects: Ubiquitous Networking between Humans and Objects, in *Proc. of the 4th International Conference on Advanced Infocomm Technology (ICAIT*), July 11–14, 2011, Wuhan, China, 588–592.
24. LIU, J.; XIAO, Y.; PHILIP. C. L. (2012). Authentication and Access Control in the Internet of Things, in *Proc. of the 32nd International Conference on Distributed Computing Systems Workshops,* June 18–21, 2012, Macau, China, 588–592.
25. LI, S.; XU, L. D.; ZHAO, S. (2015). The Internet of Things: A survey, *International Journal of Information Systems Frontiers* 17(2): 243–259.
26. MA, R.; LIU, Y.; SHAN, C.; ZHAO, X. L.; WANG, X. A. (2015). Research on Identification and Addressing of the Internet of Things, in *Proc. of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing,* November 4–6, 2015, Krakow, Poland, 810–814.
27. MAČIULIENĖ, M. (2012). Power Through Things: Following Traces of Collective Intelligence, *Research Journal of Social Technologies* 4(1): 168–178.
28. MADAKAM, S.; RAMASWAMY, R.; TRIPATHI, S. (2015). Internet of Things (IoT): A Literature Review, *International Journal of Future Computer and Communication* 3(5): 164–173.
29. MEIDAN, Y.; BOHADANA, M.; SHABTAI, A.; GUARNIZO, J. D.; OCHOA, M.; TIPPENHAUER, N. O.; ELOVICI, Y. (2017). ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis, in *Proc. of the 32nd ACM SIGAPP Symposium On Applied Computing (SAC)*, April 4–6, 2017, Marrakech, Morocco, 506–509.
30. MIETTINEN, M.; MARCHAL, S.; HAFEEZ, I.; SADEGHI, A. R.; ASOKAN, N.; TARKOMA, S. (2017). IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT, in *Proc. of the 37th IEEE Conference on Distributed Computing Systems (ICDCS)*, June 5–8, 2017, Atlanta, Georgia, USA, 53–58.
31. MIORANDI, D.; SICARI, S.; DE PELLEGRINI, F.; CHLAMTAC, I. (2012). Internet of Things: Vision, Applications and Research Challenges, *Archival Journal of Ad Hoc Networks* 10(7): 1497–1516.
32. MITTON, N.; RYL, D. S. (2011). From the Internet of Things to the Internet of the Physical World, *Journal of Comptes Rendus Physique* 12(7): 669–674.

33. MUHIC, I.; HODZIC, M. I. (2014). Internet of Things: Current Technological Review, *Journal of Periodicals of Engineering and Natural Sciences* 2(2): 1–8.
34. NITTI, M.; PILLONI, V.; COLISTRA, G.; ATZORI, L. (2016). The Virtual Object as a Major Element of the Internet of Things: A Survey, *Journal of IEEE Communications Surveys and Tutorials* 18(2): 1228–1240.
35. PALATTELLA, M. R.; DOHLER, M.; GRIECO, A.; RIZZO, G; TORSNER, J.; ENGEL, T.; LADID, L. (2016). Internet of Things in the 5G Era: Enablers, Architecture and Business Models, *IEEE Journal on Selected Areas in Communications* 34(3): 510–527.
36. PARDAL, M. L.; MARQUES, J. A. (2010). Towards the Internet of Things: An Introduction to RFID Technology, in *Proc. of the 4th International Workshop on RFID Technology (IWRT)*, June 8–12, 2010, Madeira, Portugal, 30–39.
37. PARK, S.; ZO, H.; CIGANEK, A. P.; LIM, G. G. (2011). Examining Success Factors in the Adoption of Digital Object Identifier Systems, *Journal Electronic Commerce Research and Applications* 10(6): 626–636.
38. PERERA, C.; ZASLAVSKY, A.; CHRISTEN, P.; GEORGAKOPOULOS, D. (2013). Context Aware Computing for The Internet of Things: A Survey, *Journal of IEEE Communications Surveys and Tutorials* 16(1): 414–454.
39. ROMAN, R.; ALCARAZ, C.; LOPEZ, J.; SKLAVOS, N. (2011). Key Management Systems for Sensor Networks in the Context of the Internet of Things, *International Journal of Computers and Electrical Engineering* 37(2): 147–159.
40. SALMAN, M. A. (2014). On Identification of Internet of Things, *International Journal of Sciences: Basic and Applied Research* 18(1): 59–62.
41. SUN, Y.; BIE, R.; THOMAS, P.; CHENG, X. (2015). Theme issue on advances in the Internet of Things: identification, information, and knowledge, *Journal of Personal and Ubiquitous Computing* 19(7): 985–987.
42. SHAH, S. H.; YAQOOB, I. (2016). A Survey: Internet of Things (IoT) Technologies, Applications and Challenges, in *Proc. of the 4th IEEE International Conference on Smart Energy Grid Engineering,* August 21–24, 2016, Oshawa, Canada, 381–385.
43. TAN, J.; KOO, S. G. M. (2014). A Survey of Technologies in Internet of Things, in *Proc. of the 10th IEEE International Conference on Distributed Computing in Sensor Systems*, May 26–28, 2014, Marina Del Rey, California, USA, 269–274.

44. WEN, Y.; JINLONG, W.; QIANCHUAN, Z. (2016). Physical Objects Registration and Management for Internet of Things, in *Proc. of the 35th Chinese Control Conference,* July 27–29, 2016, Chengdu, China, 8335–8339.
45. WU, M.; LU, T. J.; LING, F. Y. (2010). Research on the Architecture of Internet of Things, in *Proc. of the 3rd International Conference on Advanced Computer Theory and Engineering,* August 20–22, 2010, Chengdu, China, 484–487.