

Daiktų interneto objektų identifikavimo metodų palyginimas

Raimundas Savukynas

Vilniaus universiteto Matematikos ir informatikos instituto doktorantas
Vilnius University, Institute of Mathematics and Informatics, Doctoral Student
Akademijos g. 4, LT-08663 Vilnius
El. paštas: raimundas.savukynas@mii.vu.lt

Virginijus Marcinkevičius

Vilniaus universiteto Matematikos ir informatikos instituto vyresnysis mokslo darbuotojas
Vilnius University, Institute of Mathematics and Informatics, Senior Researcher
Akademijos g. 4, LT-08663 Vilnius
El. paštas: virginijus.marcinkevicius@mii.vu.lt

Daiktų internetas yra integrali ateities interneto dalis, kuri apibrėžiama kaip globali ir dinaminė tinklo infrastruktūra, gebanti save konfigūruoti, pagrįsta standartiniais ir suderinamais komunikavimo protokolais, kur fiziniai ir virtualūs objektai turi identifikacines savybes, fizinius atributus, virtualias personalijas, naudoja išmaniąsias sąsajas ir tiesiogiai integruoti į vientisą informacinį tinklą. Daiktų interneto resursai ir teikiamos paslaugos yra globaliai pasiskirstę informaciniame tinkle, todėl būtina turėti metodą, leidžiantį globaliai identifikuoti išmaniuosius įrenginius, jų teikiamas paslaugas ir resursus. Paprastai identifikacija susideda iš vardų priskyrimo resursams ir resursų adresavimo mechanizmo, kad būtų galima atrasti ir pasiekti nutolusius daiktų interneto resursus. Šiuolaikiniuose tinkluose naudojamas URI, kuris globaliai identifikuoja resursą, jo tipą bei aibę lygiaverčių vardų. URI leidžia unikaliai identifikuoti fizinius objektus, esančius bet kurioje pasaulio vietoje, naudojant EPC technologiją. EPC leidžia URI naudoti ir su RFID technologija, skirta objektams žymėti ir sekti. RFID grindžiama radijo dažnio signalo naudojimu objekto žymoje esančiai informacijai įrašyti ir nuskaityti. Literatūroje ji minima kaip viena iš pagrindinių daiktų interneto identifikacijos realizavimo priemonių. Šio straipsnio tikslas yra apžvelgti ir palyginti daiktų interneto objektų identifikavimo metodus.

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

Įvadas

Išmaniųjų įrenginių apsuptis ir internetas tapo įprastu mūsų gyvenimo reiškiniu. Daugumoje gyvenimo sričių ir ūkio sektorių valdymas ir stebėjimas vyksta naudojant

internetą ir 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 ir su išmaniąja aplinka keisdami duomenimis, autonomiškai reaguoti į fizinio pasaulio įvykius bei veikti aplinką atliekant įvairius veiksmus ir teikiant paslaugas (Gubbi ir kt., 2013).

Daiktų interneto kontekste daiktu laikomas fizinio arba informacijos pasaulio objektas, kuris gali būti identifiкуotas ir integruotas į komunikacinius tinklus. Fiziniai objektai paprastai egzistuoja fiziniame pasaulyje, o informacija apie juos gaunama per stimuliuojamus ir sujungiamus jutiklius. Toks fizinis objektas, kuris įgauna komunikavimo savybių, gali jungtis į daiktų internetą. Fizinis objektas 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 naudoja išmaniąsias sąsajas ir turi unikalius identifikacijos atributus, kurie leidžia jį skaitmeniškai personalizuoti. Informacijos objektas gali būti skaitmeninis elementas, turintis tikslą, sudarytas iš duomenų eilučių ir galintis atlikti nustatytus veiksmus. Fiziniam objektui informacijos pasaulyje gali atstovauti vienas ar daugiau informacijos daiktų, o informacijos objektas gali egzistuoti ir be jokio kartu susijusio fizinio daikto (Espada ir kt., 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 visapusiškai panaudoti objektus įvairioms paslaugoms, užtikrindamas aukštus saugumo ir privatumo reikalavimus. Tikimasi, kad daiktų internetas leis sujungti į visumą tokias naujausias technologijas kaip šiuolaikinė mašina – mašinai (angl. *Machine to Machine – M2M*) komunikacija, autonominiai tinklai, duomenų analizė ir sprendimų priėmimas, saugumas ir privatumo apsauga, debesų kompiuterija su moderniomis pojūčių ir paleidimo technologijomis. Pagrindiniai daiktų interneto požymiai (Nitti ir kt., 2016):

- *sujungiamumas*: viskas gali būti sujungta su pasaulio informacijos ir komunikacijų infrastruktūra;
- *susiejamumas*: daiktų internetas gali teikti su objektais susijusias paslaugas, atsižvelgiant į tokius apribojimus kaip privatumo apsauga ir semantinė fizinių ir informacijos objektų tarpusavio darna;
- *heterogeniškumas*: daiktų interneto objektai gali būti nevienalyčiai, nes remiasi absoliučiai skirtingomis technologinėmis platformomis ir tinklais;
- *dinamiškumas*: objektų būseną gali keisti dinamiškai, nes jie užmiega ir atsibunda, įjungiami arba išjungiami, 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, mobiliųjų įtaisų, belaidžio tinklo, nanotechnologijų ir

standartinio interneto. Daiktų internetą galima laikyti ateities technologijų vizija, kai realaus pasaulio objektai tampa interneto sudedamąja dalimi, kur kiekvienas objektas yra tiksliai identifikuojamas, nustatoma jo vieta ir būseną, o pats objektas pasiekiamas tinkle. Šios naujos paslaugos ir jų išmanumas kelia daiktų interneto technologijoms aukšto lygio reikalavimus (Kraijak ir kt., 2015):

- *identifikuotas ryšys*: daiktų internetas turi užtikrinti objekto ir daiktų interneto komunikaciją, paremtą pagrindiniais daikto identifikatoriais, taip pat apimti galimą skirtingų daiktų identifikatorių, kurie būtų tvarkomi vienodai, įvairiarūšiškumą;
- *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 kartu 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 pala-

kyti privatumo apsaugą, nes kiekvienas objektas, prijungtas prie daiktų interneto, kelia daug saugumo grėsmių, 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 visi jų veiklos procesai turi būti prižiūrimi ir kontroliuojami iš visiškai skirtingų vietų.

Viena iš svarbiausių daiktų interneto problemų yra 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 šiai problemai spręsti yra sukurta gausybė identifikavimo būdų ir nuolatos ieškoma naujų bei efektyvesnių (Madakam ir kt., 2015).

Straipsnio tikslas yra apžvelgti ir palyginti esamus daiktų interneto objektų iden-

tifikavimo metodus. Pirmiausia aptariama dažniausiai šiam tikslui naudojama daiktų interneto architektūra. Paskui nagrinėjami pagrindiniai daiktų interneto elementai, objektų identifikavimo protokolai ir standartai išskirstytoms aplinkoms. Toliau apžvelgiami daiktų interneto objektų identifikavimo metodai. Pabaigoje pateikiama šių metodų palyginimo lentelė.

Daiktų interneto architektūra

Prie interneto prijungtų daiktų skaičius nuolat didėja ir prognozuojama, kad iki 2020 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 internetu turi būti įmanu susieti daugybę įvairių rūšių objektų per internetą, todėl reikalinga lanksti sluoksninė architektūra (Chen ir kt., 2014).

Iki šiol pasiūlytos daiktų interneto architektūros dar nėra tapusios etaloniniu modeliu, tačiau yra nuolat vykdomi pasauliniai projektai, kad būtų galima sukurti bendrąją architektūrą remiantis įvairiomis mokslinėmis analizėmis ir pramonės poreikiais. Vienas 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 (Khan ir kt., 2012).

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, 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, taip pat stebėti ir valdyti žemiau esančius lygmenis. Verslo lygmuo išlygina kiekvieno sluoksnio išvestį su numatytu išėjimu tam, kad būtų išplėstos teikiamos paslaugos ir išlaikytas vartotojų privatumas (Muhic ir kt., 2014).

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

Paslaugų valdymo lygmuo, arba tarpinė programinės įrangos lygmuo, sujungia



1 pav. Daiktų interneto architektūra

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 ir kt., 2012).

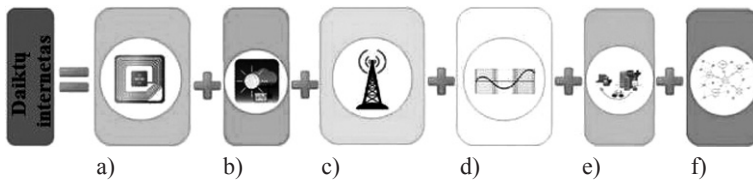
Objektų abstrakcijos lygmuo saugiais kanalais perduoda sukurtus objektų lygmens duomenis į paslaugų valdymo lygmenį. Šis lygmuo suderina prieigą prie įvairių objektų duomenų, naudodamas bendrą kalbą ir procedūras. Duomenys gali būti perduodami per tokias technologijas kaip RFID, 3G, GSM, UMTS, WiFi, Bluetooth, IR, ZigBee ir kt. Šiame lygmenyje tvarkomi duomenų valdymo procesai, debesų

Šiame lygmenyje yra priimami daiktų interneto didieji duomenys (Kuyoro ir kt., 2015).

Daiktų interneto elementai

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

Identifikavimas yra svarbus daiktų internete, siekiant pavadinti ir suderinti paslaugas su jų užklausomis. Adresuojant daiktų interneto objektus reikia diferencijuoti objekto identifikatorių nuo jo adreso. Objekto identifikatorius nurodo savo vardą jutikliui ir jo adresas per komunikacijos tinklą perduodamas į nurodytą vietą. Skir-



2 pav. *Daiktų interneto elementai:*

- a) *identifikavimas*, b) *fiksavimas*, c) *komunikacija*, d) *skaičiavimai*,
e) *paslaugos*, f) *semantika*

skaičiavimai ir kitos funkcijos (Hemalatha ir kt., 2015).

Objektų lygmuo parodo daiktų interneto fizinius jutiklius, kuriais surenkama ir apdorojama informacija. Jis apima jutiklius ir valdiklius tam, kad atliktų įvairias užklausas apie būseną, drėgmę, slėgį, svorį, vietą ir pan. Standartiškai savaiminio diegimo mechanizmams yra reikalingas sąvokos lygmuo tam, kad būtų galima sukonfigūruoti įvairius objektus. Sąvokos lygmuo skaitmenina ir saugiais kanalais siunčia duomenis į objekto abstrakcijos lygmenį.

tumas tarp objektų identifikavimo ir adresavimo yra būtinas, nes identifikavimo būdai nėra visur vienodi. Identifikavimas yra naudojamas siekiant suteikti objektams tinkle aiškia tapatybę (Choudhary ir kt., 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 konkrečius veiksmus, kurie yra grindžiami reikalingomis paslaugomis. Daiktų interneto jutikliai gali būti išmanūs priėmimo

elementai, valdikliai arba nešiojamieji fiksavimo įrenginiai (Mačiulienė ir kt., 2012).

Komunikacija daiktų internete jungia tarpusavyje įvairius objektus, 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 ir kt., 2017).

Skaičiavimus daiktų internete leidžia atlikti mikrovaldikliai ir taikomoji programinė įranga. Daugelis programinės įrangos platformų yra naudojamos teikti įvairioms daiktų interneto funkcijoms, tarp kurių 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 ir kt., 2015).

Paslaugas daiktų internete skirstomos į tapatybės nustatymo, informacijos surinkimo, bendrąsias ir universaliąsias. 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 jutiklio matavimus, kurie turi būti apdoroti ir perduoti į daiktų interneto programas. Bendrosios paslaugos veikia informacijos surinkimo paslaugų viršuje, naudoja išgautus duomenis priimdamos sprendimus ir atitinkamai reaguodamos. Universaliosios paslaugos suteikia bendrąsias paslaugas bet kuriuo metu, kai tik jos yra kam nors reikalingos. Pagrindinis daiktų interneto programų tikslas yra pasiekti universaliųjų paslaugų lygį,

tačiau tai nėra lengva, nes esama dar daug problemų, kurios ateityje turi būti išspręstos (Jia ir kt., 2012).

Semantika daiktų internete reiškia visapusišką gebėjimą išmaniai išgauti žinias iš skirtingų mechanizmų, kad būtų galima suteikti reikalingas paslaugas. Žinių gavyba apima išaiškinimą, resursų naudojimą, modeliavimo informaciją, duomenų atpažinimą ir informacijos analizavimą, siekiant suprasti teisingo sprendimo prasmę, suteikti tikslas paslaugas. Tokiu būdu semantika vaizduoja daiktų interneto intelektą siunčiant poreikius į reikiamą resursą (Gazis ir kt., 2015).

Daiktų interneto objektų identifikavimo protokolai

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

Elektroninis produkto kodas (angl. *Electronic Product Code* – EPC) yra unikalus identifikavimo numeris, skirtas fiziniams objektams identifikuoti. 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 objektus (An ir kt., 2012).

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

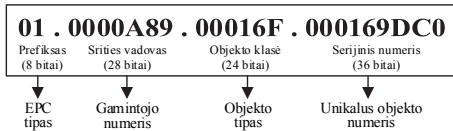
1 lentelė. *Daiktų interneto elementų technologijos*

| Daiktų interneto elementai | | Technologijos |
|----------------------------|-----------|---|
| Identifikavimas | Vardas | EPC, uCode |
| | Adresas | IPv4, IPv6 |
| Fiksavimas | | Išmanieji jutikliai, montuojamieji jutikliai, nešiojamieji 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, Nimbis, Hadoop |
| Paslaugos | | Tapatybės nustatymo, informacijos surinkimo, bendrosios, universaliosios |
| Semantika | | RDF, OWL, EXI |

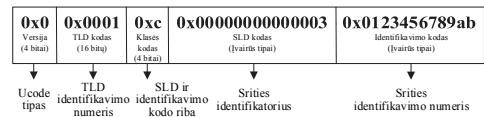
saugo 33 milijonus unikalių serijos numerių kiekvienam objekto tipui. EPC 96 bitų kodas palaiko apie 268 milijonus gamintojų su skirtingais numeriais, apima nuo 16 milijonų įvairių objektų tipų ir saugo 68 milijardus unikalių serijos numerių kiekvienam objekto tipui (Guo ir kt., 2013).

ir visiškai nepriklauso nuo taikymo srities (Gigli ir kt., 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



3 pav. *EPC struktūra*



4 pav. *Ucode struktūra*

Ucode yra unikalus identifikavimo numeris, kuris skirtas objektams, vietoms ir konceptams identifikuoti 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 specialią duomenų bazę, kuri pagal kodą gražina nuorodą į resursą. Ucode tinka identifikuoti bet kokio tipo resursus

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 domenai ir identifikuoja kiekvieną sritį. Identifikavimo kodas apibrėžia individualų tapatybės nustatymo numerį (Lee ir kt., 2011).

Interneto protokolas (angl. *Internet Protocol* – IP) yra taisyklių rinkinys, reglamentuojantis daiktų interneto objektų adresavimą, duomenų skaidymą į paketus

prieš siunčiant ir surinkimą juos atsiuntus, taip pat jų maršrutų parinkimą. IP kartu su perdavimo valdymo protokolu (angl. *Transmission Control Protocol* – TCP) sudaro TCP/IP protokolą, kuris yra pagrindinis interneto protokolas. Jis yra ir TCP/IP rinkinio adresuojantis ir maršrutizuojantis duomenis protokolas, 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 labiausiai paplitusi ketvirtoji protokolo versija IPv4, tačiau ją palaipsniui keičia naujausia, šeštoji, protokolo versija IPv6 (Atzori ir kt., 2010).

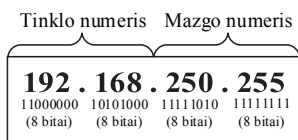
IPv4 naudoja 32 bitus adresui užrašyti, o tai apima apie 2^{32} įvairių interneto objektų. IPv4 struktūrą (5 pav.) sudaro 4 dešimtainiai skaičiai nuo 0 iki 255, kurie tarpusavyje atskirti taškais. IPv4 adresą sudaro tinklo numeris ir mazgo šiame tinkle numeris. Tinklo numeris skirtas tinklui pažymėti ir naudojamas maršrutizuojant paketus. Mazgo numeris yra priskiriamas konkrečiam tinklo objektui (Salman ir kt., 2014).

IPv6 naudoja 128 bitus adresui užrašyti, o tai apima apie 2^{128} įvairių interneto objektų. IPv6 struktūrą (6 pav.) sudaro 8 šešiolyktainiai skaičiai, kurie tarpusavyje

atskirti dvitaškiais. IPv6 struktūroje yra išskiriama tinklo ir mazgo dalis, kur 64 bitai naudojami tinklo daliai ir maršrutizavimui, o kiti 64 bitai skirti mazgui identifikuoti (Jara ir kt., 2012).

Daiktų interneto objektų identifikavimo standartai

Daugelis daiktų interneto objektų identifikavimo standartų yra sukurti siekiant palengvinti taikomųjų programų programuotojų ir įvairias paslaugas teikiančių organizacijų darbą. Šie standartai tarpusavyje skiriasi duomenų sparta, veikimo nuotoliu, energijos sąnaudomis, saugumo lygiu, naudojamų dažnių ir kitais parametrais. Daiktų interneto objektų identifikaciją palaiko tokios tarptautinių standartų kūrimo organizacijos 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 suklasifikuoti į atskiras programų, paslaugų teikimo, infrastruktūros, įtakos grupes ir pateikti 2 lentelėje (Bandyopadhyay ir kt., 2011).



5 pav. IPv4 struktūra



6 pav. IPv6 struktūra

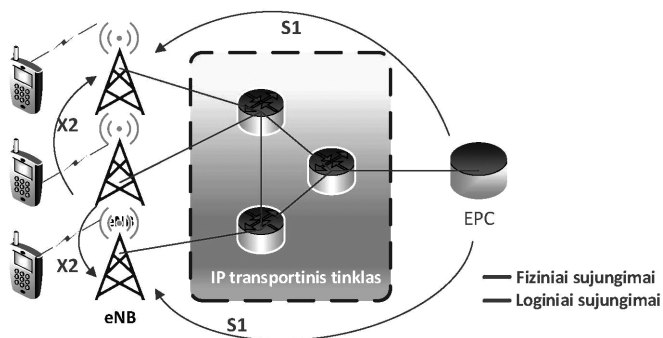
2 lentelė. *Daiktų interneto standartai*

| Programų standartai | | DDS | CoAP | AMQP | MQTT | MQTT-SN | XMPP | HTTP REST | |
|-----------------------------|-----------------|-------------|------------|---------------|-------|-----------|-------------|--------------|--|
| Paslaugų teikimo standartai | | mDNS | | | | DNS-SD | | | |
| Infrastruktūros standartai | Maršruto lygmuo | RPL | | | | | | | |
| | Tinklo lygmuo | 6LoWPAN | | | | IPv4/IPv6 | | | |
| | Ryšio lygmuo | ZigBee | | | | | | | |
| | Objektų lygmuo | LTE-A | EPC global | IEEE 802.15.4 | | Z-Wave | | | |
| Įtakos standartai | | IEEE 1888.3 | | | IPSec | | IEEE 1905.1 | | |

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 lygmeniu 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, dar vadinamas fizinių šaltinių blokais. 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 ir kt., 2017).

LTE-A tinklas (7 pav.) sudarytas iš dviejų pagrindinių sudedamųjų dalių. Pirmoji 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

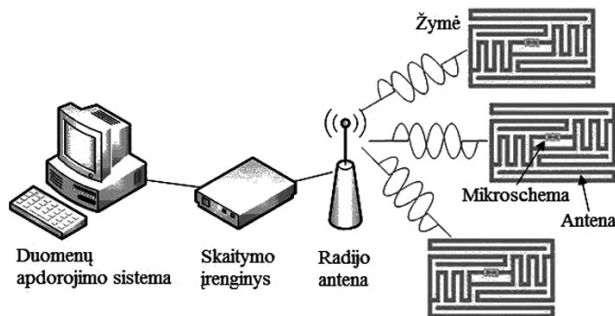


7 pav. *LTE-A tinklo struktūra*

belaidžio 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 tarpusavyje sujungtos X2 sąsajomis. RAN ir CN tarpusavyje yra sujungti S1 sąsajomis. Mobilieji arba MTC įrenginiai gali prisijungti prie bazinių stočių tiesiogiai arba per MTC vartus. Jie taip pat turi tiesioginį ryšį su kitais MTC įrenginiais (Palattella ir kt., 2016).

EPCglobal standartas aprašo EPC naudojimą žymėse ir brūkšniuose koduose, kurie įima įvairią informaciją apie nutolusius objektus. EPCglobal sistemą (8 pav.) sudaro duomenų apdorojimo sistema, skaitymo įrenginys, radijo antena, žymė su įmontuota

nedidelės duomenų perdavimo spartos, aukšto pranešimų pralaidumo, yra naudojamas IoT, M2M ir WSN. Jis suteikia patikimą ryšį, veiksmingumą tarp skirtingų platformų, valdomumą esant dideliui 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 ir platesnės dažnių juostos suteikia didelį pralaidumą ir mažą vėlinimą, nes žemesni dažniai suteikia geresnį jautrumą ir padengia didelius atstumus (Roman ir kt., 2011).



8 pav. EPCglobal sistemos struktūra

mikroschema ir nedidele antena, kurią galima pritvirtinti prie objekto, o informaciją nuskaityti radijo dažnio atpažinimo aparatūra. Nuotolinis žymės identifikavimas suteikia gamybos, logistikos, prekybos ir kitoms įmonėms plačias sistemos pritaikymo galimybes (Pardal ir kt., 2010).

IEEE 802.15.4 standartas skirtas sujungti belaidžių jutiklių tinklams (angl. *Wireless Sensor Network – WSN*), kurie yra nedidelių funkcinių galimybių. Dėl šio standarto charakteristikų – mažų energijos sąnaudų,

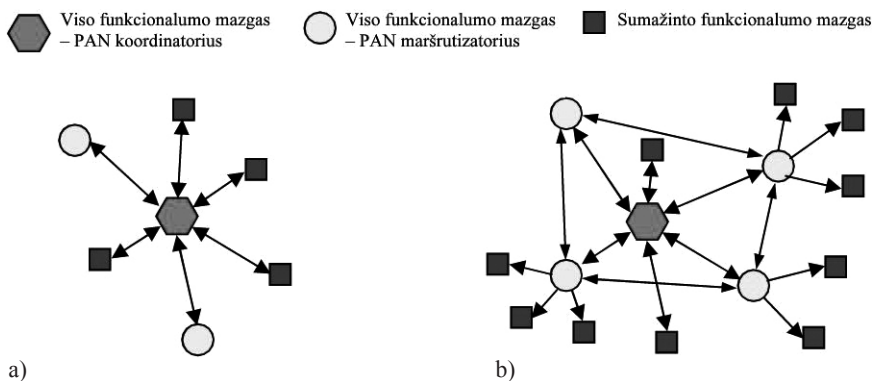
IEEE 802.15.4 standartas palaiko viso funkcionalumo (angl. *Full Function Device – FFD*) ir sumažinto funkcionalumo (angl. *Reduced Function Device – RFD*) tinklo mazgus. RFD mazgas paprastai priima ir siunčia jutiklio duomenis. FFD mazgai gali būti asmeninės erdvės tinklo (angl. *Personal Area Network – PAN*) koordinatoriai, maršrutizatoriai arba paprasti mazgai. PAN tinklo koordinatorius yra pagrindinis tinklo mazgas, kuris kuria tinklą, priima į jį kitus mazgus ir sinchronizuoja jų veikimą. Marš-

rutizatoriai gali surinkti duomenis iš kitų mazgų ir perduoti kitam maršrutizatoriui ar koordinatoriui. 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 šiame tinkle nenaudojami maršrutizatoriai. Topologijos iš mazgo į mazgą tinkle naudojami maršrutizatoriai, kurie yra komunikavimo tarpininkai, galintys persiųsti vienų mazgų pranešimus kitiems mazgams (Li ir kt., 2015).

Mažos galios belaidžio ryšio komunikacijos Z-Wave standartas yra skirtas namų automatizacijos tinklams (angl. *Home*

Daiktų interneto objektų identifikavimo metodai

Daiktų internete įvairūs objektai yra pasiskirstę aplinkoje, todėl būtina turėti tam tikrą mechanizmą, kuris leistų identifikuoti ir atrasti vienas nuo kito nutolusius daiktų interneto įrenginius. Daiktų interneto objektų identifikavimo metodai leidžia vartotojams interaktyviai sąveikauti su asmeniniais daiktais, turinčiais identifikatorius, ir gauti šiuolaikines paslaugas. Prie tokių yra priskiriami radijo dažnio identifikavimo (angl. *Radio Frequency Identification – RFID*), bendro resursų identifikavimo (angl. *Uniform Resource Identification – URI*) ir



9 pav. IEEE 802.15.4 tinklo topologijos:

a) žvaigždinė, b) iš mazgo į mazgą

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 ir kt., 2014).



10 pav. Z-Wave tinklo struktūra

skaitmeninio objekto identifikavimo (angl. *Digital Object Identification – DOI*) metodai (Meidan ir kt., 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 saugomas duomenų bazėje. RFID metodas nuskaito duomenis, saugomus objekto žymoje, naudodamas tris pagrindinius dažnių diapazonus (Kim ir kt., 2014):

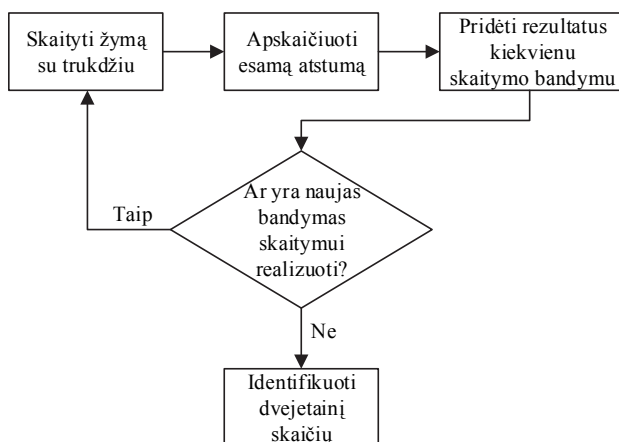
- 13,56 MHz aukšto dažnio diapazonas (angl. *High Frequency – HF*), pasižymintis trumpu žymės duomenų nuskaitymo atstumu;
- 860–960 MHz ultraaukšto dažnio diapazonas (angl. *Ultra High Frequency – UHF*), galintis nuskaityti žymės duomenis vidutiniu atstumu;
- 2,45 GHz superaukšto dažnio diapazonas (angl. *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 ko-

das, 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 pridodamas. Sprendimas atlikti didesnę skaičių bandymų yra ankstesnės duomenų apdorojimo posistemės konfigūracijos rezultatas su galimomis parinktimis (Escobar ir kt., 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 skaičių bandymų, grindžiamų apskaičiuotais skirtumų atstumais, kur bandymai baigiasi, kai skirtumas tarp minimalios sumos ir likusių sumų pasiekia iš anksto numatytą toleranciją.

URI metodas yra naudojamas fizinių arba informacijos daiktų interneto objek-



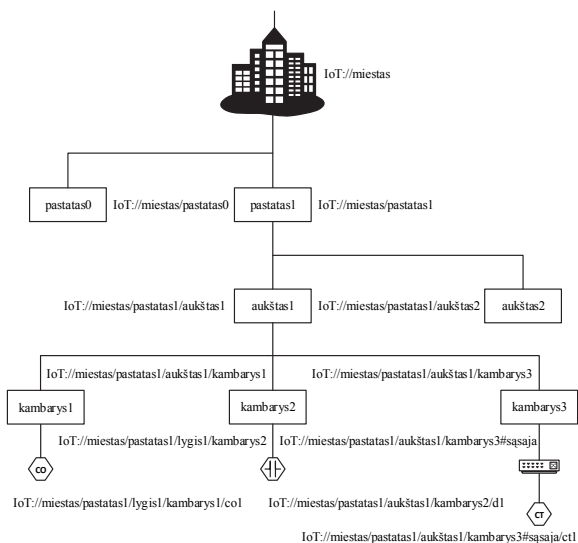
11 pav. **RFID metodas**

tams identifikuoti. Jį sudaro simbolių seka iš amerikietiškos informacijos mainų koduotės standarto. URI metodas susideda iš daiktų interneto simbolių ir tęsiamas po dvitaškio. Du pasvirieji brūkšniai nurodo kelią, kuris yra koduojamo objekto loginis adresas. Kelio seka yra atskiriama pasviraisiais brūkšniais ir toliau aprašomos fizinių objektų erdvinės vietos. Šąsaja yra atskirta nuo ankstesnės dalies grotazyme bei atskinga už jutiklių sujungimą su internetu. Objekto identifikacinis numeris nurodo fizinio objekto vardą ir gali būti sudarytas iš įvairių raidžių, kurių derinys turi būti unikalus (Ma ir kt., 2015).

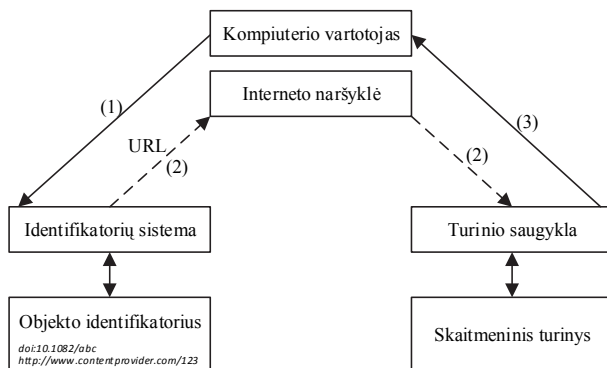
URI metodas (12 pav.) charakterizuoja visame tinkle esančius fizinius objektus pagal medžio hierarchiją. Aikštė nurodo medžio šakninį mazgą, toliau esantis lygmuo reiškia pastatą, o visi kiti lygmenys žymi pastato grindis ir kambarius. Pirmame kambaryje įrengtas dūmų jutiklis, antrame kambaryje sumontuotas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

DOI metodas yra naudojamas daiktų interneto objektams identifikuoti skaitmeninėje erdvėje. Jį sudaro simbolių seka iš priešdėlio ir priesagos, kurie tarpusavyje yra atskirti pasviruoju brūkšniu. Priešdėlis yra katalogo ir registravimo kodų tarpusavyje 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 ilgio ir kitų sudedamųjų dalių, kurios yra visuotinai unikalios, apribojimų (Park ir kt., 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* –



12 pav. URI metodas



13 pav. DOI metodas

3 lentelė. RFID, URI, DOI metodų palyginimas

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

URL) su papildomais metaduomenimis. Antrame etape į pateiktą kompiuterio vartotojo užklausą grąžinamas atsakymas 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 ir kt., 2016).

Daiktų interneto identifikavimo metodų palyginimui yra naudojama stiprybių, silpnybių, galimybių, grėsmių (angl. *Strengths, Weaknesses, Opportunities, Threats* – SWOT) analizė, kurios rezultatai pateikiami 3 lentelėje.

Išvados ir siūlymai

1. Daiktų internetas yra neatskiriama ateities interneto dalis, kuri apibrėžiama kaip pasaulinė ir dinaminė tinklo inf-

rastruktūra, gebanti save konfigūruoti, 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, todėl siūloma sukurti universalius daiktų interneto objektų identifikavimo protokolus ir standartus.
3. Daiktų internetas apibrėžia išmanią aplinką, kurioje fiziniai daiktai įgauna tarpusavio komunikavimo galimybes ir tiesiogiai integruoti į vientisą informacinį tinklą, kuriame daiktai tampa aktyvūs verslo procesų dalyviai, todėl siekiant daiktų interneto objektų tarpu-

savio komunikacijos siūloma sukurti daiktų interneto objektų identifikavimo metodą.

4. Daiktų interneto identifikacijos protokolų ir standartų apžvalga parodė, kad šias technologijas galima suskirstyti į centralizuotas identifikacijos technologijas, naudojančias centrinę duomenų bazę identifikuojamų objektų metaduo-
menims saugoti ir paskirstytas identifi-
kacijos sistemas, kuriose informacija apie daiktų interneto objektų teikiamas

paslaugas ir resursus yra paskirstyta daiktų interneto mazguose.

5. Daiktų interneto objektų identifikavimo metodų apžvalga ir palyginimas parodė, kad prieigos kontrolė leidžia apsaugoti daiktų interneto objektų duomenis, kad nebūtų nesankcionuoti naudojami, ir leidžia informaciją pasiekti tik igalio-
tiems vartotojams.

Tolesnių tyrimų tikslas – pasiūlyti ir tobulinti multimodalinio daiktų interneto objektų identifikavimo ir autentifikavimo metodo prototipą.

LITERATŪRA

- AL-FUQAHA, A.; GUIZANI, M.; MOHAMMADI, M.; ALEDHARI, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *International Journal of IEEE Communications Surveys and Tutorials* 17(4): 2347–2376.
- AN, J.; GUI, X. L.; HE, X. (2012). Study on the Architecture and Key Technologies for Internet of Things. In *Proc. of the 7th International Conference on Electrical and Computer Engineering (ICECE)*, December 20–22, Dhaka, Bangladesh, p. 329–335.
- ATZORI, L.; IERA, A.; MORABITO, G. (2010). The Internet of Things: A Survey. *International Journal of Computer and Telecommunications Networking* 54(15): 2787–2805.
- 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.
- 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.
- 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, Jaipur, India, p. 1–8.
- DANILOV, K. N.; KULIK, V. A.; KIRICHEK, R. V. (2016). Review and Analysis of Methods of Identification and Authentication of the Internet of Things Devices. *Science Journal of Information Technology and Telecommunications* 1(3): 49–57.
- 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.
- 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.
- 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, Dubrovnik, Croatia, p. 1090–1095.
- GIGLI, M.; KOO, S. (2011). Internet of Things: Services and Applications Categorization. *Journal of Advances in Internet of Things* 1(2): 27–31.
- 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.
- 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.
- 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, Guiyang, China, p. 2797–2801.

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.

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.

JIA, X.; FENG, Q.; FAN, T.; LEI, Q. (2012). RFID Technology and its Applications in Internet of Things (IoT). In *Proc. of the 2th International Conference on Consumer Electronics, Communications and Networks (CECNet)*, April 21–23, Yichang, China, p. 1282–1285.

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, Islamabad, Pakistan, p. 257–260.

KOCAKULAK, M.; BUTUN, I. (2017). An Overview of Wireless Sensor Networks Towards Internet of Things. In *Proc. of the 7th Annual Computing and Communication Workshop and Conference (CCWC)*, January 9–11, Las Vegas, Nevada, USA, p. 1–6.

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 (ICCT)*, October 18–20, Hangzhou, China, p. 28–31.

KUYORO, S.; OSISANWO, F.; AKINSO-WON, 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, London, United Kingdom, p. 53–58.

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, Wuhan, China, p. 588–592.

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, Macau, China, p. 588–592.

LI, S.; XU, L. D.; ZHAO, S. (2015). The Internet of Things: A survey. *International Journal of Information Systems Frontiers* 17(2): 243–259.

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, Krakow, Poland, p. 810–814.

MAČIULIENĖ, M. (2012). Power Through Things: Following Traces of Collective Intelligence. *Research Journal of Social Technologies* 4(1): 168–178.

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.

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, Marrakech, Morocco, 506–509.

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 International Conference on Distributed Computing Systems (ICDCS)*, June 5–8, Atlanta, Georgia, USA, p. 53–58.

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.

MUHIC, I.; HODZIC, M. I. (2014). Internet of Things: Current Technological Review. *Journal of Periodicals of Engineering and Natural Sciences* 2(2): 1–8.

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.

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.

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, Madeira, Portugal, p. 30–39.

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.

PERERA, C.; ZASLAVSKY, A.; CHRISTEN, P.; GEORGAKOPOULOS, D. (2013). Context Aware Computing for The Internet of Things: A Survey. *International Journal of IEEE Communications Surveys and Tutorials* 16(1): 414–454.

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.

SHAH, S. H.; YAQOUB, 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 (SEGE)*, August 21–24, Oshawa, Canada, p. 381–385.

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, Marina Del Rey, California, USA, p. 269–274.

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, Chengdu, China, p. 8335–8339.

A COMPARISON OF THE IDENTIFICATION METHODS OF OBJECTS OF THE INTERNET OF THINGS

Raimundas Savukynas, Virginijus Marcinkevičius

S u m m a r y

The Internet of Things is an integral part of the future Web part, which is defined as a global and dynamic network infrastructure, which is capable of self-configuring and is based on standardized and compatible communications protocols, where physical and virtual objects have identification characteristics, physical attributes, virtual personalities that use intelligent interfaces and are directly integrated into the unified information network. The resources of the Internet of Things and services are globally distributed within the information network, so it is necessary to have a mechanism which allows the identification of global smart devices, their services and resources. Typically, the identification consists of the assigning names for the resources and the mechanism of the addressing resources in order to discover and access the remote resources of the Internet of things. Modern networks

use the Universal Resource Identifier (URI), which identifies a global resource, its type and a set of equivalent names. The URI uniquely allows to identify physical objects, which are located anywhere in the world, using the Electronic Product Code (EPC) technology. EPC allows URI to also be used with Radio-Frequency Identification (RFID). The RFID technology is used for marking and tracing items, which is based on the use of the frequency signal of the radio in the object tag for information recording and reading. This technology in literature is mentioned as one of the main identification and realization measures of the Internet of Things. The purpose of this article is to review and compare the identification methods of objects of the Internet of Things.

Keywords: internet of things, objects identification, future internet, internet services, smart devices.

Iteikta 2017 m. liepos 10 d.