KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

Marius Karotkis

DAIKTŲ INTERNETO PROTOKOLŲ SAUGOS IR ENERGIJOS SĄNAUDŲ TYRIMAS

Baigiamasis magistro darbas

Vadovas
Prof. dr. A. Venčkauskas

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

TVIRTINU
Katedros vedėjas
(parašas) Prof. dr. Algimantas Venčkauskas
(data)

DAIKTŲ INTERNETO PROTOKOLŲ SAUGOS IR ENERGIJOS SĄNAUDŲ TYRIMAS

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) Prof. dr. Algimantas Venčkauskas
(data)

Recenzentas
(parašas) Prof. Rimantas Plėštys
(data)

Projektą atliko
(parašas) Marius Karotkis
(data)

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos

(Fakultetas)

Marius Karotkis

(Studento vardas, pavardė)

Informacijos ir informacinių technologijų sauga, 621E10003

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Daiktų interneto protokolų saugos ir energijos sąnaudų tyrimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 ___ m. _____ ____ d.

Kaunas

Patvirtinu, kad mano **Mariaus Karotkio** baigiamasis projektas tema „Daiktų interneto protokolų saugos ir energijos sąnaudų tyrimas“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

_____ _____

(vardą ir pavardę įrašyti ranka) *(parašas)*

Karotkis, M. Daiktų interneto protokolų saugos ir energijos sąnaudų tyrimas. Magistro baigiamasis projektas / vadovas Prof. dr. A. Venčkauskas; Kauno technologijos universitetas, informatikos fakultetas, kompiuterių katedra.

Kaunas, 2015. 45 psl.

SANTRAUKA

Darbo tikslas - išanalizuoti daiktų interneto protokolus, jų saugumo lygius, bei atlikti energijos sąnaudų tyrimą.

Analitinėje darbo dalyje analizuojami mobilūs tinklai, jų architektūros, galimos konfigūracijos, taikymas ir saugos problemos. Palyginamos bevielių tinklų specifikacijos. Antroje dalyje analizuojamos komunikacinių protokolų modeliavimo priemonės, jų galimybės tirti komunikacinius protokolus, jų elgsenas ir jas atvaizduoti. Modelis turėtų atspindėti esamo ar planuojamo sprendimo savybes ir apibrėžti numanomą funkcionalumą, kad būtų kuo mažiau nenumatytų grėsmių. Trečioje dalyje aprašomas tyrimo modelis, kokios priemonės naudojamos modelio kūrimui ir tyrimo atlikimo eiga. Eksperimentinė dalyje pateikiami rezultatai ir išvados, apibendrinančiomis tyrimo rezultatus, bei tyrimo metu padarytos įžvalgos.

Nustatyta, kad ZigBee bevielio ryšio tinklas tinka ten kur nereikalauja didelės duomenų perdavimo spartos. Toks tinklas gali būti saugus, o baterijos, kurios maitina mazgus, ilgai veikia, nes vienas iš svarbiausių ZigBee tinklų prioritetų yra energijos taupymas. Bevielis ZigBee tinklas gali turėti iki 65535 įrenginių. Todėl toks tinklas tinkamas daiktų internetui.

SUMMARY

Subject of the work is to perform analysis of the internet of things protocols on their security and energy consumption levels.

Mobile networks analysis is performed in the analytical part of this work. Networks are analyzed by researching their architecture, possible configurations and security risks in real world applications. Part two involves research of the communication protocol modeling tools and their ability perform communication protocol analysis by investigating protocol behavior and modeling them visually. Model in question should be able to represent existing or future solutions precisely. This way possibility to avoid future risks becomes higher. Third part is oriented towards the modeling and tools that were used in the process.

The results are presented in the experimental part. This summarizes research and insights that were made in the process. ZigBee wireless communication network can be used in the situations where low power consumption is required and the data transfer speed of low priority. The network is relatively safe and the batteries that supplies power to the network nodes should work for the long time. ZigBee network can have up to 65535 devices. These are the main advantages of the ZigBee network over the similar solutions and so it is possible to use it in the internet of things.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

Terminas	Paaiškinimas
PAN (angl. personal area network)	Asmeninės erdvės tinklas
FFD (angl. full-function device)	Viso funkcionalumo įrenginys
RFD (angl. reduced-function device)	Sumažinto funkcionalumo įrenginys
WSN	Mobilus sensorinis tinklas
MAC (angl. Media Access Control)	Fizinis tinklo plokštės adresas. Tai yra unikalus gamintojo suteikiamas tinklo plokštės adresas
IoT (angl. Internet of Things)	Daiktų internetas
Framework	Bazinis sistemos karkasas
Firmware	Programinė aparatinė įranga, įrašyta į pastoviąją atmintį

ĮVADAS

Šis baigiamasis darbas parašytas studijuojant Kauno technologijos universitete, Informacijos ir informacinių technologijų saugos studijų programą.

Darbo problematika ir aktualumas

IT prietaisų ir įrenginių apsupti, bei internetas tapo įprastu reiškiniu mūsų gyvenime -– nuo išmaniųjų telefonų ar kompiuterių, kuriuos nuolat naudojame, iki jutiklių ir prietaisų, kurių nepastebime, bet jie supa mus kasdien. Daiktų internetas (angl. IoT arba Internet of Things) gali būti suprantamas kaip globalioji infrastruktūra, teikianti pažangias paslaugas, sujungiant tiek fizinius ir tiek virtualiuosius daiktus besivystančių ir esamų informacinių ir ryšių technologijų pagrindu. Daiktų internetas (DI) – tai kasdienių daiktų, prietaisų, kurie yra kompiuterizuoti, sujungimas į egzistuojančią interneto infrastruktūrą. Sparčiai vystantis daiktų interneto technologijoms, daugėja įrenginių, kurie jungiami į interneto tinklą, t.y. mobilūs įtaisai, jutikliai, valdikliai ar buitiniai prietaisai. Daiktų interneto vystymasis priklauso nuo daugelio kitų inovacinių technologijų. Praktiškai visose gyvenimo srityse valdymas ir stebėsena vyksta naudojant internetą ir skaitmeninius prietaisus, veikiančius per interneto tinklą. Duomenys per tinklą perduodami ne tik sąveikaujant žmogui su žmogumi ar žmogui su kompiuteriu, bet ir per jutiklius sąveikaujant įrenginiui su įrenginiu. Daiktų internetas kaip ir kiekviena kuriama technologija, pirmiausia turi palengvinti ir pagerinti žmonių gyvenimą, todėl nauda neabejotina. Žingsnis po žingsnio kompiuterinė technika skverbiasi į mūsų kasdieninį gyvenimą, prognozuojama, kad iki 2020 metų daiktų kurie bus prijungti prie interneto, skaičius išaugs nuo šiuo metu naudojamų 15 milijardų iki 50 milijardų. Jau šiuo metu savo namo valdymą patikime namų valdymo sistemoms, kurios valdo šildymą, vėdinimą, apšvietimą ir kt. Tokios sistemos kaupia duomenis, stebi vartotojo įpročius ir norus, bei juos analizuoja, kad reikiamu laiku priimtų sprendimus.

Internete vienas iš didžiausių iššūkių yra saugumas, tai liečia ir daiktų internetą. Įvairioms sistemoms renkant informaciją apie vartotojo veiksmus, būtina užtikrinti informacijos konfidencialumą ir vientisumą. Saugumui nuolat ieškoma naujų sprendimų, kuriama gausybė metodų, ieškoma vis efektyvesnių. Saugumui užtikrinti galima naudoti gerai žinomus sprendimus: ugniasienė, VPN, SSL/TLS. Bet naudojant mobilius įtaisus iškyla dar viena problema, jie veikia esant ribotiems resursams, tiek skaičiavimo tiek ir energijos. Skaičiavimo resursus galima prognozuoti ar numatyti iš anksto, o energijos prognozavimas sudėtingesnė problema.

Informacijos apsauga, šifravimas ir iššifravimas didina energijos sunaudojimą, pvz. SSL protokolo panaudojimas padidina energijos sunaudojimą iki 15%, toks padidėjęs energijos vartojimas mobiliems įrenginiams yra didelė problema. Daugėjant elektros įrenginių išauga didėjantis elektros energijos poreikis, išauga poreikis tokiems protokolams kurie naudoja mažiau energijos.

Darbo tikslas ir uždaviniai

- Ištirti daiktų interneto protokolų saugos lygio, energijos sąnaudų tarpusavio ryšį ir priklausomybę nuo aplinkos sąlygų.
- Išanalizuoti naudojamus populiarius/esamus daiktų interneto protokolus;
- Ištirti ZigBee protokolo energijos suvartojimą naudojant ir nenaudojant saugius protokolus;

Darbo rezultatai ir jų svarba

Tyrimo metu ištirta ZigBee protokolo energijos sąnaudų tarpusavio ryšio ir priklausomybės nuo aplinkos sąlygų ir saugumo. ZigBee bevielio ryšio tinklai tinka ten kur nereikalauja didelės duomenų perdavimo spartos. Toks tinklas gali būti saugus, o baterijos, kurios maitina mazgus, ilgai veikia, nes vienas iš svarbiausių ZigBee tinklų prioritetų yra energijos taupymas.

Darbo struktūra

Darbas sudarytas iš šių pagrindinių dalių

1. Daiktų interneto bevielio ryšio protokolų analizė
2. Modeliavimo priemonių analizė

3. Tiriamo modelio sudarymas
4. Eksperimento dalis

Pirmoje dalyje pateikiama mobiliųjų tinklų analizė, architektūros, duomenų perdavimo protokolai, jų saugos problemas ir energijos suvartojimas. Pasirenkamas ZigBee protokolas, kurio energijos suvartojimas bus tiriamas.

Antroje dalyje analizuojamos komunikacinių protokolų modeliavimo priemonės, jų galimybės tirti komunikacinius protokolus, jų elgsenas ir jas atvaizduoti.

Trečioje dalyje aprašomas tyrimo modelis, kokios priemonės bus naudojamos ir kaip atliekami skaičiavimai.

Eksperimentinė dalyje pateikiami rezultatai, ir išvados, apibendrinančiomis tyrimo rezultatus, bei tyrimo metu padarytos įžvalgos.

1. ENERGIJĄ TAUPANČIŲ KOMUNIKACINIŲ PROTOKOLŲ SAUGOS REIKALAVIMŲ ANALIZĖ

Šioje dalyje bus analizuojami bevieliai tinklai, jų saugos lygiai ir elektros energijos suvartojimas.

1.1. Analizės tikslas

Analizės tikslas nustatyti ir apibrėžti daiktų interneto (DI) protokolų modeliuojamus parametrus.

1) Daiktų interneto sąvoka, bei veikimo principas.
2) Daiktų interneto plačiausiai nagrinėjami objektai.
3) Daiktų interneto saugių protokolų ir energijos suvartojimo problema.

1.2. Daiktų interneto tinklo topologijos

Šiame skirsnyje analizuojama esamos mobiliųjų tinklų architektūros ir jų galimos konfigūracijos, bei taikymas, kad kitame skirsnyje būtų galima analizuoti duomenų perdavimo protokolus ir saugos problemas siekiant apibrėžti modeliuojamus daiktų interneto protokolų parametrus.

Tinklai gali būti statiniai, dinaminiai ir mobilūs. Bendroji daiktų interneto tinklo topologija yra hierarchinė ir gali turėti daug lygmenų. Galimi įvairūs topologijos variantai: vienas su vienu (angl. point-to-point arba P2P), vienas su daugeliu (angl. point-to-many arba P2M), daug su daug (angl. many-to-many arba M2M). Duomenų perdavimas yra vienas iš esminių atributų, užtikrinančių daiktų interneto funkcionalumą, o mobilumas perduodant duomenis įgauna vis didesnį mastą, todėl tikslinga nagrinėti mobilių tinklų sąsajas su daiktų internetu ir jų galimybes.

Žemiau lentelėje pateikiami galimi mobilaus ryšio tinklai ir jų bendrosios charakteristikos: architektūros ir topologijos, bei taikymai. Žemiau pateikta Lentelė sudaryta remiantis šaltinio [1] analize. Šiame šaltinyje nagrinėjama mobiliųjų tinklų saugumo problemas nepriklausomai nuo daiktų interneto konteksto. Pagal rastus literatūroje duomenis (saugumą, taikymus, publikacijų kiekį ir kt.) galima spręsti, koks mobilus tinklas labiausiai tikėtinas daiktų interneto taikymuose.

Lentelė 1.1 Mobiliųjų tinklų tipai, architektūra ir taikymai pagal Chen ir Zhang [1]

Mobilaus tinklo tipas	Architektūra ir topologija	Taikymai	Pastabos
Bluetooth	Palaiko ryšį tarp bet kurių įtaisų, kuriuose yra įdiegtas Bluetooth aparatinis modulis su programine įranga (išmanieji telefonai, PK, skaitmeninės kameros ir kt.)	Suprojektuotas pagal mažos energijos ir žemos komunikavimo kainos kriterijus. Priklausomai nuo versijos gali pateikti ryšį 10-100 m. atstume su 700 Kb/s, 2.1 Mb/s, ar iki 24 Mb/s duomenų perdavimo greičiu.	Nenaudoja standartinių IP pagrindu saugumo protokolų tokių kaip SSL/TLS, digital certificates, ar IPSec.
CNW	Korinio ryšio architektūra su bazinėmis stotimis 10 - čių km. spinduliu; (P2P)	Kasdieninė veikla: Gauti, skaityti, siųsti informaciją, naršyti internete, valdyti sąskaitas ir pan.	
MANET	Mobilūs spontaniški tinklai	Literatūra nenagrinėja specifinių taikymų ir daroma prielaida, kad jie identiški ar	Didžioji dalis literatūros nagrinėja energijai

		tapatūs tiems, kuriuos įgalina internetas.	efektyvius protokolus.
RFID	RFID technologiją sudaro maži nebrangūs skaičiavimo įtaisai su bevielio komunikavimo funkcija.	Pagrindinis taikymas - fizinių prekių tiekimas ir apskaita. Naudojamos prekių etiketės (angl. tags) su skaičiavimo-komunikavimo funkcija. Jas galima laikyti brūkšninio kodo pakaitalu.	
VANET	Daug su daug, transporto priemonė su keliu. Dinaminė topologija su besikaitaliojančiu ryšiu laike.	Intelektualios transporto sistemos.	Energijos problema jiems neegzistuoja.
WLAN	Prieigos taškas (AP- Access Point) iki 100 m	Kasdieninė veikla: Gauti, skaityti, siųsti informaciją, naršyti internete, valdyti sąskaitas ir pan.	Dažniausiai priklauso vienai organizacijai.
WMAN	Ryšys palaikomas 3-48 km diapazone.	Remiasi IEEE 802.16 standartu , komercinis pavadinimas WiMAX (angl. Worldwide Interoperability for Microwave Access). Pateikia priemones sujungti optiniais kabeliais vietinius tinklus. Skirtas didelėms organizacijoms, individams ir kartais viešoms paslaugoms	Apima didelius miestus ar dideles stovyklas.
WMN	WMN yra WLAN junginys. Apibūdinamas trimis pagrindinėmis sąvokomis: tinklo klientas (PK, mob. telefonas); maršrutizatorius ir vartai (tiesioginis ryšys su internetu)	Skirtas pakeisti laidinius tinklus įvykus katastrofoms. Remiasi IEEE 802.11 standartu. IEEE 802.11 yra bevielio ryšio standartų šeima (įvairios versijos: (802.11b/802.11g/802.11n)	
WSN	Dinaminė topologija	Karyba, aplinkos stebėjimas, pavojų valdymas, medicina, vandenynų stebėjimas ir t.t. 1. Daug objektų (1000); 2.Komunikavimo dažnis ir energija – esminiai apribojimai; 3 Dinaminė topologija; 4. Neturi globalių identifikatorių;	Kai kuriuose straipsniuose minimas kaip potencialiai naudotinas daiktų internetui.

CNW – (Cellular Networks) korinio ryšio tinklai;
WLAN - bevieliai vietiniai tinklai;
MANET - (Mobile Ad hoc network) mobilūs spontaniški tinklai;
VANET - (Vehicular Ad Hoc Networks) auto-transporto spontaniški tinklai;
WSN - (Wireless Sensor Networks) bevieliai sensorių tinklai;

WMN - (Wireless Mesh Network) bevielis hibridinis tinklas;

RFID - (Radio Frequency Identification) radio dažnio identifikacija.

Šaltinis [Labiod, et al., 2007] architektūrinius mobiliųjų (bevielių) tinklų aspektus nagrinėja kur kas išsamiau ir sisteminčiau. Komunikavimas įvairiuose tinkluose yra paremtas standartų IEEE802.11 šeimyna. Knygoje [Labiod, et al., 2007] detaliai aprašomas tos šeimynos struktūra/ architektūra, funkcionalumas. Ši standartų šeimyna dar vadinama Wi-Fi, Bluetooth, WiMAX, ir ZigBee. Todėl, remiantis tuo šaltiniu, galime pateikti mobiliųjų tinklų architektūrų taksonomiją ir taikymus.

1.3. Spontaniški (Ah hoc) tinklai ir jų protokolai

Mobilūs Ad Hoc tinklai (angl. Mobile Ad Hoc networks) tai judantys įrenginiai sujungti tarpusavyje bevielio ryšio jungtimis. Galima išskirti į dvi Ad Hoc tinklų veikimo rūšis: taškas-taškas (angl. point-to-point) ad hoc, kai įrenginiai tiesiogiai komunikuoja vienas su kitu ir daugelio žingsnių (angl. Multi-hop) ad hoc - kai tinklo įrenginiai gali komunikuoti tarpusavyje kitų tarpinių mazgų pagalba. įrenginiai Ad Hoc tinkle vienu metu turi būti informacijos ir siuntėjai ir gavėjai, turi veikti kaip maršrutizatoriai, persiunčiantys kitų įrenginių paketų srautą. Tokiam tinklui reikalingi maršrutų parinkimo protokolai optimaliai maršrutų paieškai. Ad Hoc tinkle esantys mazgai juda laisvai, todėl topologija keičiasi. Maršrutizavimo protokolai Ad Hoc tinkluose yra lentelėmis paremti (angl. table-driven) statiniai ir šaltinio inicijuojami (angl. source-initiated) dinaminiai. Statiniai maršrutizavimo protokolai laiko informaciją apie viso tinklo topologiją ir nuolat siunčia atnaujinimo paketus, kad atnaujinti turimą informaciją. Informacija surenkama ir paskleidžiama tinkle kai atsiranda naujas įrenginys ar nutrūksta sujungimas. Statinių maršrutizavimo protokolų greitis yra didesnis, nei dinaminio, tačiau dideliam tinklui sunkiai spėjama atnaujinti informaciją, o atnaujinimo paketai užimą didelę dalį tinklo pralaidumo. Dinaminiuose maršruto parinkimo protokoluose maršrutas sudaromas kai atsiranda poreikis persiųsti informaciją. Šaltinis norintis persiųsti informaciją inicijuoja kelio suradimo procesą, o tarpiniai taškai maršrutų lentelėse informaciją apie kelią saugo tik kol tas kelias yra naudojamas. Dinaminiuose protokoluose kelio suradimas užtrunka ilgiau, bet jie geriau susitvarko esant tinklo topologijos pasikeitimams.

Plečiamumas (Scalability). Tinklo savybė nusakanti, kad tinklas gali būti plečiamas, t.y. paslauga gan kokybiškai teikiama dideliam taškų skaičiui. Statiniai protokolai netinkami didelio mobilumo aplinkose, nes reikalingas didelis srautas tarnybiniams duomenims vykstant pasikeitimams. Dinaminiai protokolai leidžia kurti didelius tinklus, tačiau didėja maršruto užklausų atsako laikas.

Paslaugos kokybė (angl. Quality of Service). Ryšio perdavimo kokybė apibrėžiama parametrais: duomenų perdavimo pralaidumas (angl. overhead), perdavimo vėlinimas (angl. delay), paketų praradimo koeficientas (angl. loss rate), maršruto suradimo laikas, palaikymas.

Saugumas. Saugumas Ad Hoc tinkluose yra kritinė problema, nes tokiame tinkle nėra centralizuoto tinklo valdymo. Naudojant viešo rakto infrastruktūrą atsiranda plečiamumo ir energijos naudojimo efektyvumo problemos. Galimas saugus maršrutizavimas kai informacija skaidoma į daug dalių ir siunčiama skirtingais maršrutais.

Energetinis efektyvumas. Ad Hoc tinkluose dažniausiai naudojami įvairūs mobilūs įrenginiai, telefonai, kompiuteriai, specializuoti moduliai transporto priemonėse ir kt.. Tokių įrenginių skaičiavimo galimybės dažniausiai būna labai ribotos, ir tokie įrenginiai dirbantys pilnu pajėgimu greičiau išnaudoja baterijos energiją. Kiekvienas įrenginys, keičiasi su kitais įrenginiais informacija, taip pat turi veikti kaip maršrutizatorius, kad palaikyt kitų įrenginių komunikaciją per jį, tokiu atveju procesorius reikalingas maršrutų skaičiavimui, ryšio užmezgimui, jo palaikymui, saugumo algoritmų raktų perdavimui. O taip pat ir fizinio lygmens sprendimams palaikyti, tokiems kaip bevielio tinklo plokštės galingumo reguliavimui, miego režimui kai ji nenaudojama ir kt.

1.4. IEEE 802.15.4

IEEE 802.15.4 standartas skirtas belaidžio ryšio mazgams sujungti, kurie turi nedideles funkcines galimybes ir sunaudoja mažai energijos. Dažniausiai tokie tinklo mazgai maitinimą gauna iš elementų, kurių jiems turėtų užtekti apie metus, be įkrovimo ar keitimo. IEEE 802.15.4 standarto pirmoji versija buvo paskelbta 2003 metais. Standarte aprašomas fizinis lygmuo, kuris trumpiau vadinamas PHY, bei duomenų kanalo lygmuo, trumpiau žymimas MAC. Su IEEE 802.15.4 ir aukštesniuosius OSI lygmens aprašomais standartais (ZigBee ir kt.) galime kurti didelius belaidžių jutiklių tinklus.

Tinklo mazgai skirstomi į du tipus:

- Viso funkcionalumo (FFD)
- Sumažinto funkcionalumo (RFD)

RFD mazgas priima ir siunčia jutiklio duomenis, o FFD mazgai gali būti PAN tinklo koordinatoriai, maršrutizatoriai ar paprasti mazgai. Pan tinklo koordinatorius yra pagrindinis tinklo mazgas, kuris sukurią tinklą, bei priima kitus mazgus į jį, taip pat prižiūri tinklo veikimą. Maršrutizatoriai surenka duomenis iš kitų mazgų ir perduoda kitiems maršrutizatoriams ar koordinatoriui.

IEEE 805.15.4 standartas numato dvi topologijas: žvaigždinę ir iš mazgo į mazgą (P2P). Žvaigždinėje topologijoje visi taškai komunikuoja su koordinatoriumi, nenaudojat maršrutizatorių. Topologijoje iš mazgo į mazgą naudojami maršrutizatoriai, reikalingi komunikacijos tarpininkavimui, gali persiųsti vienų iš vienų mazgų informaciją į kitus mazgus.

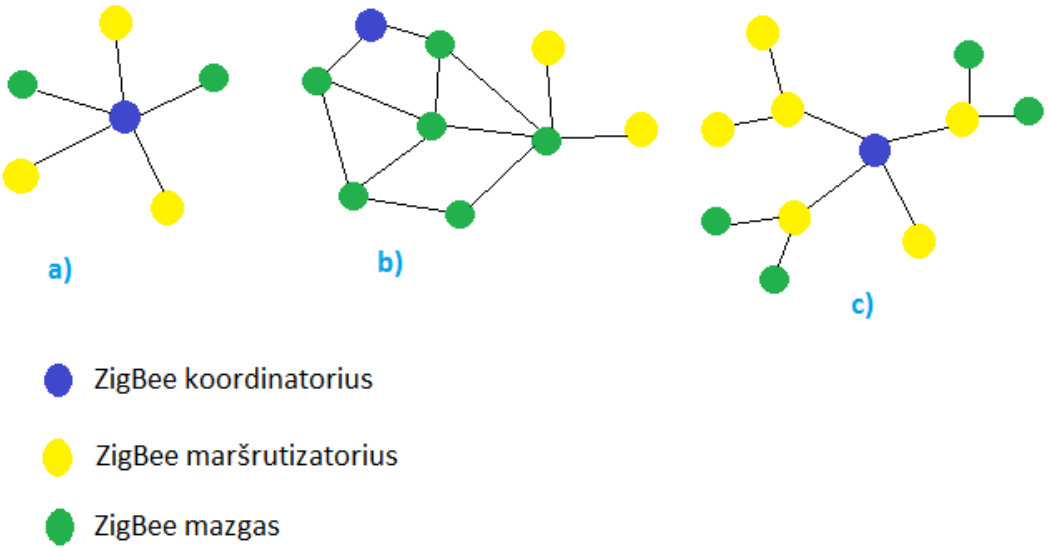
1.5. ZigBee

ZigBee specifikacija aprašo belaidžio tinklo protokolus, kuriame yra naudojami mažos galios mazgai. Specifikacija aprašo tinklo ir taikomąjį lygmenis, naudodamasi, kad duomenų perdavimo kanalo ir fizinis lygmuo yra kuriami pagal standartą IEEE 802.15.4. Šis tinklas tinka ten kur nereikalauja didelės duomenų perdavimo spartos. Toks tinklas gali būti saugus, o baterijos, kurios maitina mazgus, ilgai veikia, nes vienas iš svarbiausių ZigBee tinklų prioritetų yra energijos taupymas. ZigBee specifikacijas kuria ir publikuoja ZigBee aljansas, specifikacija nekomerciniais tikslais viešai prieinama ZigBee aljanso internetinėje svetainėje. Standartas apibrėžia duomenų perdavimo spartas: 20 Kb/s; 40 Kb/s; 100Kb/s; ir 250 Kb/s. Pasauliniu mastu naudojamas 2,4 GHz dažnių ruože.

ZigBee veikimo atstumas tarp įrenginių iki 10m, bet gali veikti ir iki 100m, jei naudojama mažesnė perdavimo sparta.

ZigBee tinklo topologijos

ZigBee tinklo lygmenyje gali būti įrenginys-įrenginys, žvaigždinė, medžio ir tinklo topologijos.



Pav. 1.1 ZigBee tinklo topologijos: a) žvaigždinė, b) medžio, c) tinklo

Žvaigždinėje topologijoje tinklą kontroliuoja vadinamas ZigBee tinklo koordinatorius, kuris sukuria tinklą ir prijungia kitus mazgus prie savęs, o kiti mazgai yra galiniai mazgai, kurie tiesiogiai komunikuoja su koordinatoriumi. Medžių ir tinklo topologijose koordinatorius taip pat atsakingas už tinklo sukūrimą, kuriame jis parenka pagrindinius tinklo parametrus, bet šie tinklai gali būti praplėsti naudojant maršrutizatorius. Tinklo arba P2P galimi visi sujungimai tarp mazgų, ribojami tik atstumai.

Bevielis ZigBee tinklas savo topologijoje gali turėti iki 65535 šakų. Energijos taupymą realizuoja savybė, kai mazgas nenaudojamas jis pereina į taupymo režimą. Taupymo režime nenaudojamas mazgas sunaudoja labai mažai energijos, o jį „pažadinus“ iškart galima siųsti ir priimti duomenis, darbui pasibaigus vėl pereinama į energijos taupymo režimą.

ZigBee saugumas

ZigBee protokolas remiasi „pasitikėjimo centro“ koncepcija, kai tinklas turi pasitikėjimo centrą. Šis centras sukuria tinklą ir paskirsto raktus, pasitikėjimo centras vadinamas koordinatoriumi. Tinklą sudaro koordinatorius, maršrutizatoriai ir mazgai.

Saugos charakteristikos:

Naujumas: įrenginiai palaiko įeinančių ir išeinančių naujumo skaitiklius, kad užtikrintų duomenų naujumą. Skaitikliai atnaujinami kiekvieną kartą, kai sukuriamas raktas. Įrenginiai, kurie perduoda duomenis kartą per sekundę, neperpildys jų naujumo skaitiklio 136 metus.

Pranešimų vientisumas.

Apsauga užtikrina nuo pranešimo pakeitimo perduodant informaciją. Norint užtikrinti vientisumą galima naudoti 0, 32, 64, 128 bitus. Standartinė numatoma reikšmė yra 64 bitai. Vientisumo rėžimai (variantai) įgalina nustatyti pusiausvyrą tarp pranešimo vientisumo apsaugos ir pranešimo pertekliškumo.

Autentiškumas.

Autentiškumas užtikrina pranešimo šaltinio kilmę. Autentiškumas galimas tinklo ir prietaiso lygmenyse. Tinklo autentiškumas pasiekiamas naudojant bendrą tinklo raktą (reikalauja šiek tiek atminties). Prietaiso autentiškumas pasiekiamas naudojant unikalius raktus tarp įtaisų porų (reikalauja daugiau atminties).

Šifravimas.

Apsauga nuo galimybės perklausyti pranešimą. Apsauga galima tinklo ir prietaiso lygmenyje, naudojant 128 bitų AES šifravimą. Šifravimas gali būti išjungtas be poveikio kitoms apsaugos rūšims (autentiškumui, vientisumui ir atstatymui) nepaveikiant. ZigBee architektūra turi protokolo saugumą NWK, APS lygmenims ir naudoja 802.15.4 MAC lygmens apsaugą.

MAC lygmens apsauga. MAC lygmens kadrams apsaugoti, ZigBee naudoja MAC lygmens apsaugą, kuri nurodyta 802.15.4 protokolo specifikacijoje. Ši apsauga naudojama siekiant apsaugoti MAC lygmens komandas, žymes ir patvirtinimo kadrus. MAC lygmenyje naudojamas šifravimas AES, kaip pagrindinis šifravimo algoritmas. Paveiksle vaizduojama ZigBee kadro struktūrą su apsaugos sritimis. MAC lygmenyje kartu su MAC antrašte pridedama pagalbinė antraštė. Pranešimo vientisumo žymė (MIC) nustato vientisumo lygį, žymės vertės gali būti 0, 32, 64 ir 128.

Pav. 1.2 MAC lygmens apsaugos pavaizdavimas ZigBee kadre

NWK lygmens apsauga. Žemiau pateiktas paveikslas rodo saugumo sritis, kurios yra naudojamos NWK lygmens kadro apsaugai užtikrinti. NWK lygmenyje prie NWK antraštės pridedama pagalbinė antraštė. Duomenų vientisumo lygį nustato MIC žymė.

Pav. 1.3 NWK lygmens apsaugos pavaizdavimas ZigBee kadre

APL lygmens saugumas. APS lygmens kadrų apsauga pagrįsta sujungimo arba tinklo raktais. Paveiksle matosi APS lygmenyje kartu su APS antrašte pridedama ir pagalbinė antraštė. Taip pat naudojama duomenų vientisumo lygį nustatanti MIC žymė.

Pav. 1.4 APL lygmens apsaugos pavaizdavimas ZigBee kadre

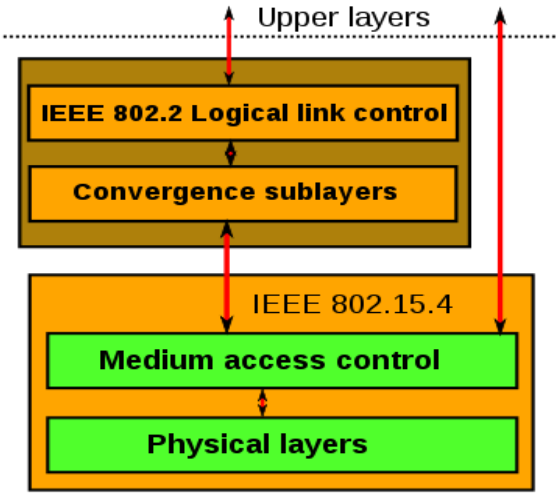
Apibendrinant ZigBee protokolas pateikia gerus saugos sprendimus, kai tenkina trumpas atstumas ir mažas greitis, bevielėms sistemoms.

1.6. Energijos sunaudojimo problemos

Standartizavimo organizacijos siūlo nedidelės energijos komunikavimo technologijas. Plačiau žinomos yra tokios:

1) IEEE 802.15.4 - žemos kainos, mažai energijos suvartojanti, palyginti nesudėtingas protokolas skirtas sujungti apribotų resursų įtaisus fiziniame ir duomenų ryšio lygiuose (t.y., 1 ir 2 sluoksniuose pagal OSI).

Bendra standarto IEEE 802.15.4 architektūra pavaizduota žemiau paveiksle. Bazinė struktūra apima iki 10 metrų komunikavimo diapazoną su 250 Kb/s perdavimo greičiu ir žvaigždės topologija.



Pav. 1.5 Komunikavimo standarto IEEE 802.15.4 struktūra

Svarbios savybės: tinkamumas realaus laiko sistemoms numatant garantuotus laiko intervalus operacijoms ir kolizijų išvengimui ir integruotos saugaus komunikavimo priemonės. Jungiami prietaisai turi energijos valdymo funkcijas. Perdavimo dažnis gali būti keičiamas siekiant mažinti energijos suvartojimą.

2) Bluetooth bevielė duomenų perdavimo technologija, kuri naudoja mažai energijos. Bluetooth LE (angl., LE- Low energy) - tai Bluetooth technologijos ultra žemos energijos versija, kuri iki 15 kartų efektyvesnė nei standartinė technologija.

Žemiau lentelėje pateikiamas bazinės Bluetooth ir Bluetooth LE technologijų techninių charakteristikų palyginimas:

Lentelė 1.2 Dviejų technologijų charakteristikų palyginimas [Jara et al., 2013].

Techniniai parametrai	Bluetooth 2.1	Bluetooth LE
Radio dažnis	2.4 GHz	2.4 GHz
Padengiamas nuotolis	~10-100 m	~50 m
Simbolių perdavimo greitis	1-3 Mb/s	1 Mb/s
Taikymo našumas	0.7-2.1 Mb/s	305 kb/s
Jungiamų viršūnių skaičius (slaves)	7	Neribotas
Saugos raktų ilgis	6 - 128 bitai	128 bitai AES
Technologijos naujumas (*robustness*)	FHSS*	FHSS*
Paslėptas veikimas (*sleep to send*)	>100 ms	<3 ms
Balso galimybė	Taip	Ne
Energijos sąnaudos	1 (reference)	0.01 to 0.5 (use case)
Piko srovės sąnaudos	<30 mA	<18 mA
Topologija	Išsibarstęs (*Scatternet*)	žvaigždė
Paslaugos suradimas	Taip	Taip
Taikymo profiliai	Taip	Taip
Protokolai	9 (RFCOMM, SDP, etc.)	1 (Attribute)
Valdomi pranešimai	75 LMP pranešimai	8 LL valdomi pranešimai
Paketų tipai	5 (privalomi)	2 (reklama / duomenys)

* FHSS-Frequency Hopping Spread Spectrum

3) UWB plačiajuostė technologija (angl., Ultra-Wide Bandwidth) pritaikyta daiktų internetui, įgalinanti perduoti signalus didesniame dažnio diapazone nei standartinės

sistemos. Be to, UWB turi galimybes sujungti didesnio tikslumo prietaisus daiktų interneto taikymuose.

Energijos taupymo problema mobiliuose sensoriniuose tinkluose turi savo specifiką. Pavyzdžiui, siekiant mažinti energijos suvartojimą, yra naudinga naudoti įvairias grupavimo schemas, apjungiant tinklo tarpines viršūnes. Straipsnis [6] nagrinėja hierarchiškai sugrupuotą bevielį tinklą, kad būtų galima minimizuoti energijos sunaudojimą surenkant duomenis.

Kitame šių autorių straipsnyje [6] nagrinėjama energijos taupymo problema dviejuose lygmenyse: MAC (Medium Access Control) ir tinklo sluoksnyje, bei siūlomas energijos sąnaudų priderinimo algoritmas.

Apibendrinimui galima teigti, kad mažesnis energijos suvartojimas mobiliuosiuose įtaisuose (mobiliuosius įtaisus viso projekto kontekste galima laikyti internetiniais daiktais) užtikrinant saugų komunikavimą gali būti pasiektas įvairiais būdais: a) pritaikant specialius protokolus; b) pridedant prie protokolų tam tikrus saugumą palaikančius elementus; c) perkeliant saugumo problemos sprendimą iš fizinio į taikomąjį lygmenį; d) sukuriant specializuotą įrangą kriptografijos operacijoms. Toliau aptariami detaliau paminėti sprendimai.

Kamel [8] siūlymas yra sudaryti saugumo protokolus mobiliosioms aplinkoms, remiantis nesaugių protokolų versijomis, pritaikant programinio saugumo komponentus ir kiekvieną papildyti tam tikra saugumo savybe. Iškeldami saugos funkcionalumus į aukštesnį (išorinį) lygmenį ir pritaikydami saugumo laipsnį vartotojo poreikiams, šio straipsnio autoriai pateikia saugios vadybos architektūrą adaptuotą mobilioms aplinkoms.

Prasithsangaree ir Krishnamurthy [9] pateikia pakankamo saugumo koncepciją , kuri numato saugumo lygmenis ir saugos paslaugas, esant minimaliam energijos suvartojimui. Taip pat jie pateikia saugos karkasą, kuris sudarytas iš trijų metodų efektyviam (energijos atžvilgiu) saugos protokolui sukurti. Pirmasis siūlo saugos algoritmą pakeisti kitu, kuris suvartoja mažiau energijos. Antrasis siūlo standartinių protokolų modifikaciją tam, kad pasiekti mažesnį energijos suvartojimą. Trečiasis metodas siūlo „tuščio lauko“ (greenfield) principą, kai iš principo kuriama nauja sistema, paremta energiją taupančiais saugiais protokolais.

Cano ir Domenech-Asensi [11] pateikia saugų, energijai efektyvų sprendimą mobiliems įtaisams. Saugumas užtikrinamas taikymo sluoksnyje pritaikius įvairias saugumo strategijas, priklausomai nuo duomenų, kurie turi būti siunčiami taupant atitinkamą resursą. Jų siūlomas sprendimas nereikalauja nuolatinės internetinės prieigos: paketai bus siunčiami tik tada, kai bus būtina, taip bus taupomas ryšio kanalas ir baterija.

Tam, kad būtų galima pagerinti saugios komunikacijos apdorojimo efektyvumą įterptiniuose įtaisuose, [12] siūlo naudoti įterptinius procesorius. Jie tiria bendrą poveikį tiek kriptografiniams algoritmams tiek protokolų apdorojimui: 1) konfigūruojant architektūrinius parametrus (procesoriaus instrukcijas, duomenų greitosios atminties (cache) dydį, procesoriaus atminties sąsajos plotį įterptinių procesorių); 2) išplečiant bazines instrukcijas, t.y. įvedant specializuotas instrukcijas, pritaikytas efektyviam kriptografinių algoritmų ir protokolų apdorojimui.

Kriptografiniuose algoritmuose labai aktuali kriptografinių raktų generavimo problema. Straipsniuose [Venčkauskas et al., 2012], [Venčkauskas et al., 2012A] siūloma kriptografinius raktus generuoti panaudojant programinius generatorius priderinant juos prie įtaisų charakteristikų. Tačiau tokie sprendimai nėra pakankamai lankstūs ir efektyvūs esamiems internetiniams taikymams, kadangi reikia perprogramuoti sistemos ne tik kliento, bet ir serverio dalies programinę įrangą, o taip pat reikalauja papildomos aparatūros įrangos.

Pagal padarytą apžvalgą, jau seniau žinomus internetinių technologijų sprendimus bandoma pritaikyti jutiklių tinklams, kurie sudaro daiktų interneto pagrindą. Todėl SSL protokolas taip pat taikytinas daiktų interneto panaudos kontekste.

Mokslininkai A. V. Taddeo ir A. Ferrante sprendė problemą [10] kaip realiu laiku pasirinkti atitinkamą kriptografinį algoritmą atsižvelgiant į saugos keliamus reikalavimus ir likusius sistemos resursus. Autorių pateikta metodika, pagal kurią realiame laike galima pasirinkti atitinkantį kriptografinį algoritmą. Ši metodika paremta trimis kriptografinio algoritmo veiksniais: laiko, atminties ir energijos sąnaudomis. Energijos sąnaudos gali būti ne tik paskaičiuotos iš anksto, bet ir nustatomos realiu laiku. Pirmas variantas tinka greitai ir paprastai metodikos integracijai, antras

variantas realiu darbo metu. Tikrindami metodiką autoriai rėmėsi iš anksto nustatytomis kriptografinių algoritmų resursų galimomis sąnaudomis. Šiame tyrime buvo naudojami labai tikslūs matavimo įrankiai ir energijos sąnaudos gautos mikro-džaulių tikslumu, rezultatus matome resursų sąnaudų lentelėje žemiau.

Lentelė 1.3 Resursų sąnaudos

Šifravimas	Rakto ilgis	Bloko dydis	Duomenų atmintis	Programos atmintis	Iniciavimo laikas	Laikas	Iniciavimo energija	Energija
	Bitai	Baitai	Baitai	Baitai	µs	µs /baitas	µJ	µJ/ baitas
3DES CBC	168 + 24	80	10244	142272	31,52	1,08	363,91	12,27
ARC4	128	-	8192	73424	16,27	0,08	248,99	1,7
AES CBC	256	80	20932	123488	61,61	0,17	1094,75	2,28

Po tyrimo autorių padarytos išvados:

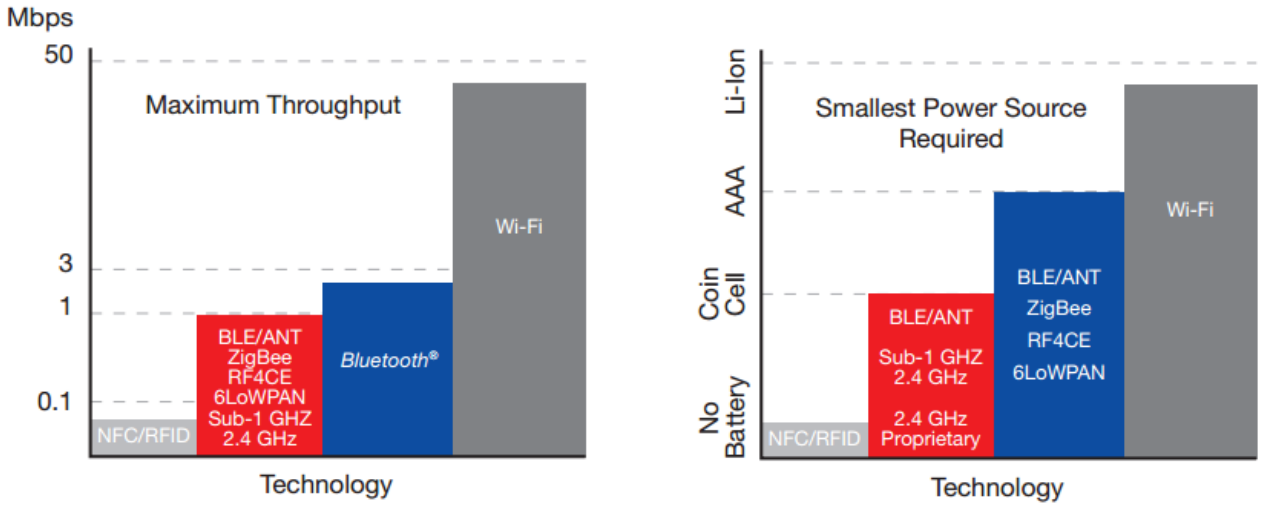
a) Tipinis sprendimo priėmimo uždavinys yra optimalaus kriptografinio algoritmo parinkimas;

b) Kaip pirminis veiksnių įvertinimo algoritmas yra pasirinktas analitinis hierarchinis procesas;

c) Pagal poreikius ir galimybes pasirenkamas optimaliausias algoritmas;

d) Norint tęsti darbus reikia sukurti prototipą ir išbandyti siūlomą metodą realiomis sąlygomis.

Žemiau paveiksle matome bevielių tinklų palyginimą pagal duomenų perdavimo greitį (Mbps) ir pagal reikalingus energijos resursus.



Pav. 1.6 bevielių protokolų palyginimas[1]

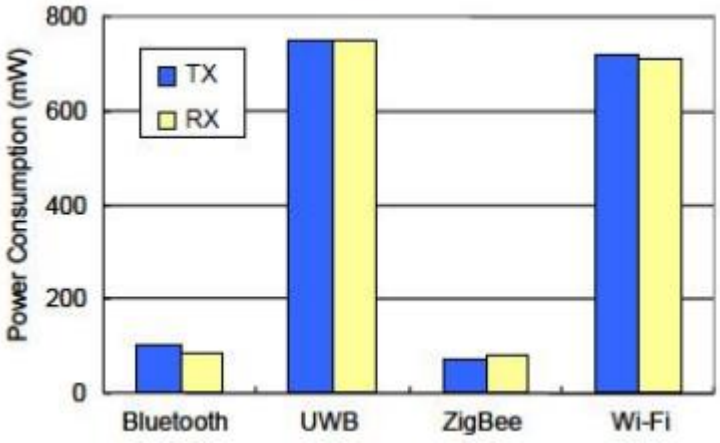
[1] http://www.ti.com/lit/sg/slab056d/slab056d.pdf

ZigBee and other wireless technologies

Market Name Standard	ZigBee™ 802.15.4	GSM/GPRS CDMA/1xRTT	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1
Application Focus	Monitoring & Control	White Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB	1MB	16KB
Battery Life (days)	100 - 1,000	1 - 7	.5 - 5	1 - 7
Network Size	Unlimited	1	32	7
Bandwidth (KB/s)	20 - 250	124 - 68	11,000	720
Transmission Range (meters)	1 - 100	1,000	1 - 100	1 - 10
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

Pav. 1.7 Įmonės Schneider Electric bevielių tinklų palyginimas[2]

Karunakar Pothuganti ir Anusha Chitneni straipsnyje palyginami duomenų perdavimo protokolai Bluetooth, UWB, ZigBee, ir Wi-Fi. Žemiau pateiktame paveiksle matomas bevielių protokolų energijos sunaudojimo palyginimas siunčiant duomenis ir juos gaunant.



Pav. 1.8 Energijos sunaudojimo palyginimas siunčiant ir gaunant duomenis

Pagal šiuos palyginimus galima teigti, kad kai reikia mažų energijos sąnaudų ir užtenka nedidelės duomenų spartos, ZigBee bevielis tinklas yra optimaliausias.

[2] http://www2.schneider-electric.com/documents/support/white-papers/40110601_Zigbee_EN.pdf

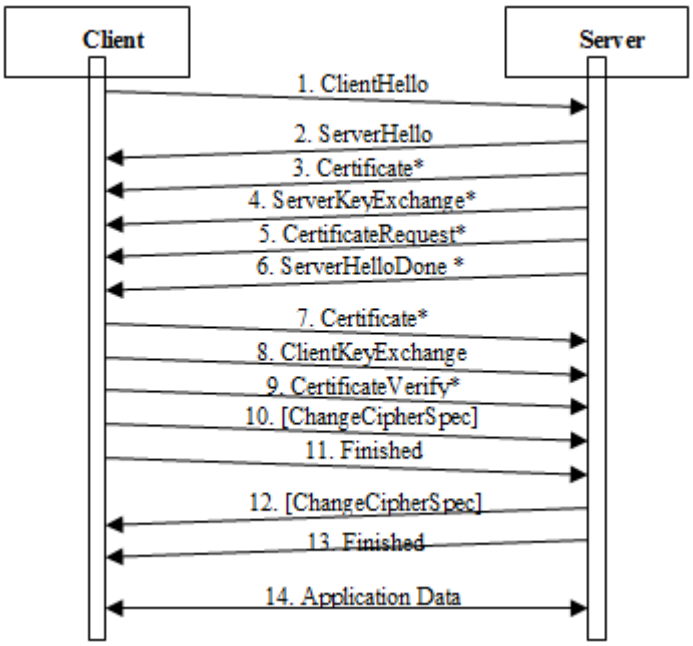
1.7. SSL/TLS saugos protokolas

SSL/TLS – kriptografinis protokolas, naudojamas apsaugoti perduodamą informaciją tarp serverio ir kliento, bendraujančių TCP protokolu, ją šifruojant. Šis protokolas naudoja tiek simetrinį, tiek asimetrinį šifravimą. SSL/TLS užtikrina perduodamos informacijos autentiškumą, vientisumą, konfidencialumą, bei nuo paketų pakartojimo atakų. Šis protokolas skirtas apsaugoti perduodamiems duomenims tarp dviejų tinklo taškų, todėl negalima naudoti transliuojamų pranešimų (angl. Multicast/Broadcast) apsaugai.

SSL/TLS protokolo realizacija nepriklauso nuo operacinės sistemos, nes jis veikia virš transporto sluoksnio. Šis protokolas susideda iš keturių protokolų:

- Šifravimo pakeitimo protokolo;
- Įspėjimų (alert) protokolas;
- Rankos paspaudimo protokolas;
- Įrašo protokolas.

Toliau aprašomas SSL protokolo funkcionalumas, kuris pavaizduotas bazinių operacijų sekos paveiksle. Sesijos kriptografiniai parametrai sukuriami patvirtinimo protokolo 1 – 13 žingsniuose. SSL klientui ir serveriui pradėjus komunikuoti, jie sutaria dėl protokolo versijos, pasirenka kriptografinius algoritmus, pasirinktiniai identifikuoja vienas kitą ir apsikeičia šifravimo raktu. Klientas suformuoja pranešimą (ClientHello), per kurį perduodamas serveriui šifravimo įrankių sąrašas (CipherSuite), kuris turi eilę kriptografinių algoritmų, pateikiamų kliento surikiuota tvarka (pirmas algoritmas pasirenkamas pirmuoju). Kiekvienas šifravimo įrankis apibrėžia rakto apsikeitimo algoritmą, saugios maišos funkciją ir suspaudimo algoritmą. Serveris pasirenka šifravimo įrankį.



Pav. 1.9 Patvirtinimo veiksmai tarp kliento ir serverio

*Priklausomai nuo situacijos pasirenkamas pranešimas, kuris ne visada siunčiamas

Patvirtinimo seansui pasibaigus, klientas ir serveris gali pradėti taikymo duomenų apsikeitimą (14 žingsnis). Klientas sukuria galimų kriptografinių algoritmų sąrašą. Kiekvienas algoritmas turi skirtingą saugos užtikrinimo lygį, be to, reikalauja skirtingų skaičiavimo ir energijos

resursų. Taigi, vartotojui egzistuoja galimybė pasirinkti optimaliausią variantą tarp saugos laipsnio ir reikalaujamų resursų. Ši idėja gali būti pritaikoma adaptuojant ir pritaikant SSL protokolą.

Skirtingiems saugos tikslams, skirtingi saugos lygmenys. Norint patenkinti saugos tikslus, turi būti parenkami atitinkami kriptografijos metodai. Pavyzdžiui, užtikrinus konfidencialumą, SSL naudoja skirtingų raktų ilgių simetrinius algoritmus duomenims užšifruoti. Energijos suvartojimas ir kriptografijos algoritmų greitis gali būti matuojamas naudojant įvairius metodus ir įrankius [Toldinas, 2011]. Tam tikslui naudojami Microsoft Research Joulemeter matavimo įrankiai [22].

1.8. Išvados

1. Informacijos sauga ir energijos suvartojimas, tai technologijų problemos, kurios nėra naujos ir tebeegzistuoja tiek interneto, tiek mobilių technologijų sprendimuose. Ypač šios problemos išryškėja daiktų internete, kai resursai yra riboti.
2. Informacijos apsaugos lygiai priklauso nuo šifravimo algoritmo raktų ilgio, todėl toks parametras labai svarbus atliekant tyrimus su energijos sąnaudomis daiktų internete.
3. Nustatyta, jog tyrėjai tyrinėdami daiktų interneto problemas ir iššūkius, remiasi pasiekimais ir rezultatais, kurie jau buvo pasiekti technologijose, kurias daiktų internetas paveldi (t.y. internetas, mobiliosios technologijos, kriptografiniai sprendimai ir kt.).
4. Lyginant bevielius tinklus galima teigti, kad kai reikia mažų energijos sąnaudų ir užtenka nedidelės duomenų spartos, ZigBee bevielis tinklas yra optimaliausias.
5. Pagal išanalizuotus daiktų interneto protokolus ir jų saugą, energijos sąnaudos priklauso nuo saugos mechanizmų, pasirenkamų kriptografinių algoritmų ir aplinkos sąlygų. Todėl toliau bus analizuojama įvairių charakteristikų matavimo metodikos ir atliekamas energijos sąnaudų nustatymo tyrimas, naudojant skirtingus apsaugos lygius ir aplinkas.

2. KOMUNIKACINIŲ PROTOKOLŲ MODELIAVIMO PRIEMONIŲ ANALIZĖ

Daiktų interneto protokolus, kaip ir belaidžius tinklus galime tirti naudojant įvairius modeliavimo metodus: imitacinis, fizinis, hibridinis modelis ir kt. Dažniausiai yra naudojamas imitacinis modeliavimas.

Sistemų imitacinis modeliavimas. Sistemos modelis - abstrakti sistema, skirta analizuoti jos elgseną, bei ją atvaizduoti. Sistemos modeliavimas padeda lengviau suprasti sistemos funkcionalumą. Modeliai yra abstraktūs ir nėra aprašoma sisteminė informacija. Formaliais metodais aprašomi būsimi modeliai.

Techninės ir programinės įrangos modeliavimas yra aktuali problema įvairioms technologijoms. Modelis turėtų atspindėti esamos ar planuojamos sistemos savybes ir apibrėžti numanomą funkcionalumą. Modelio kūrimo eiga turi būtinai remtis formaliu aprašymu. Matematinis modelis turėtų artėti link idealaus elgsenų eiliškumo, sistemos procesų veikimo lygiagretumo ir ryšių tarp funkcinių modulių. Kai kurie modeliai yra numatomi sistemos duomenų srautams apdoroti, o kiti labiau taikomi valdymui, ar apjungia duomenų srautų apdorojimą, bei jų valdymą.

Pagal sudarytą modelį kuriama imituojančios programos, kurios imituoja modelio elgseną. Sugeneruotos modelio elgsenos yra apdorojamos nustatant modeliuojamų modelio charakteristikų statistinius įverčius.

Yra sukurta daugybė įvairių priemonių skirtų imitacinių modelių kūrimo automatizavimui. Šias priemones galime skirstyti į grupes: probleminiai sričiai orientuotos imitacinio modeliavimo sistemos, bendros paskirties imitacinio modeliavimo sistemos (pvz. GPSS, ARENA ar SIMSCRIPT), tokios sistemos kaip telekomunikacinių tinklų imitacinio modeliavimui Ns-2, OPNET , OMNet++ ir imitacinių modelių sudarymo priemonės naudojančios sistemų formalius aprašymo metodus tai Petri tinklai, DEVS, SDL, PLA.

Bendros paskirties modeliavimo kalbų trūkumas yra tas, kad ne visada leidžia tiesiogiai adekvačiai aprašyti sudėtingesnius funkcionavimo algoritmus, analizuojamose sistemose. Tam reikalinga sukurti papildomus programinius modelius, kuriuos reikėtų įtraukti į pagrindinę imitatoriaus programą.

Tinklų imitacines programas galima skirstyti į keletą grupių: pagal protokolus, technologijas, bei apdorojimo metodus, taip pat ir pagal imitavimo metodus. Pagrindiniai du imitatorių kūrimo metodai yra naudojami tokie: diskrečių įvykių ir analitinis imitavimas. Dažnai šie metodai yra naudojami kartu, tai užtikrina priimtiną modelio greitaveiką ir pakankamą tikslumą.

OPNET sistemoje kuriami baigtinių būsenų modeliai ir juos apjungiant su analitiniais modeliais. Su OPNET galima modeliuoti įrenginius, protokolus ir elgsenas, panaudojant apie 400 specialių modeliavimo funkcijų. Sistema su grafinė vartotojo sąsają.

Ns-2 yra įvykiais valdomas tinklų imitatorius. Sistema turi daugumą internetinių protokolų modelių. Tinklo imitatorius leidžia animuoti duomenų perdavimą tinkle paketų lygyje. Sistema leidžia vartotojams koreguoti tinklo protokolus, bei parametrus įvairiuose protokolų lygiuose.

OMNeT++ - atviro kodo ir atviros charakteristikos imitavimo aplinka. Ši sistema naudojama įvairių architektūrų tinklus imitaciniams modeliams kurti, bei buvo naudojama kuriant kitų internetinių protokolų imitatorius.

Imitacinių modelių programinė įranga naudojanti formalius metodus turi šiuos privalumus:

- Imitacinių modelių metodai nėra orientuoti į konkrečią probleminę sritį. Imitacinių modelių sudarymo konkretizacija atliekama pagal analizuojamos sistemos komponentų formalius aprašymus.
- Sudaryti sistemos formalūs aprašymai, pagrindžia sudaromo modelio adekvatumą ir korektiškumą.

Pasaulyje paplitęs DEVS (angl. discret event specification) metodas, šio metodo teorinius pagrindus sudaro jungtinio ir atominio DEVS modelių panaudojimas, sistemų elgsenai aprašyti. DEVS - matematinė struktūra turinti pagrindinius automatus, modelio komponentus ir papildomas funkcijas aprašančias sistemas, būsenų kaitą, kurios iššaukia vidiniai komponento procesai.

Belaidžiai sensoriniai tinklai ir jų protokolai yra modeliuojami įvairiais aspektais ir metodais bei priemonėmis.

Jin-Shyan Lee [26] straipsnyje pateikia populiarių bevielio ryšio standartų, Bluetooth, UWB, ZigBee ir Wi-Fi, tyrimą ir įvertina jų pagrindines funkcijas ir veikimą pagal įvairius rodiklius, įskaitant ryšio laiką, duomenų kodavimo efektyvumą, sudėtingumą ir energijos suvartojimą.

S.Sanaa ir Amal El Arid (S.Sanaa, 2012) staipsnyje pateikta išsamios studijos, besiremiančios mobiliųjų įtaisų energijos sąnaudų eksperimentiniais matavimais, saugaus naršymo internete metu. Taip pat įvertinamos energijos sąnaudos duomenų persiuntimo metu, bei juos šifruojant ir dešifruojant, atliekant maišą ir betarpiškai naršymo metu. O taip pat autoriai pasiūlo empirinį energijos sąnaudų saugiai naršant internete modelį, įvertinantį įvairius protokolo ir įtaiso parametrus.

Chen Shengyang ir kt. (Chen Shengyang, 2013) straipsnyje pasiūlyta eMTCP – nauja mažomis energijos sąnaudomis pasižyminti daugialypė TCP (angl. Multipath TCP) grįsto informacijos pateikimo schema, derinanti mažas energijos sąnaudas su išaugusiu pralaidumu. eMTCP pozicionuojama mobiliųjų įtaisų viršutiniame transportiniame sluoksnyje ir nereikalauja MPTCP serverio modifikacijų. eMTCP padidina mobiliųjų įtaisų energetinį efektyvumą, perkeldama srautą iš daugiau energijos sunaudojančių sąsajų į kitas. Modeliavimu grįstuose eksperimentuose naudojant eMTCP modelį duomenų srautai buvo siunčiami per 3GPP (LTE) ir IEEE 802.11 (WiFi) sąsajas ir parodė iki 14% didesnį eMTCP energetinį efektyvumą lyginant su MPTCP, ir iki 66% aukštesnę kokybę lyginant su vieno kelio TCP.

Hongwei Li ir ktstraipsnyje [25] aptariami ZigBee duomenų persiuntimo saugos servisai, šifravimo metodai, saugos raktai, saugos centras, saugus kadro formatas ir saugos lygmuo.

S.Tozlu ir M. Senel straipsnyje [27] nagrinėja Wi-Fi jutiklio sąlygojamą baterijos darbo laiką, esant duotam darbo scenarijui, ir tiria paketų dydžio, duomenų mainų spartos, programos kodo ilgio, saugos schemų ir MAC sluoksnio įtaką baterijos darbo laikui.

C.S.Malavenda ir kt. straipsnyje [28] pateikia vėlinimams pakankamų ir mažomis energijos sąnaudomis pasižyminčių protokolų, skirtų saugos taikymams bevielių jutiklių mazguose, analizę, realizaciją ir eksperimentinio testavimo rezultatus. Pateikti sprendimai naudingi daugelyje sričių, kur svarbios mažos energijos sąnaudos ir susiduriama su vientiso ir be pertrūkių pasižyminčio ryšio, kurį užtikrina bevieliai tinklai, problemomis kartu su bevielių tinklų mazgų ribotais resursais.

R. Balani (Balani Rahul, 2007) analizuoja Bluetooth, WiFi (802.11) ir korinių tinklų vidutines energijos sąnaudas, persiunčiant f baitų per sekundę sparta generuojamus duomenis. Daroma prielaida, kad duomenų paketas generuojamas kas tbuf sekundžių ir perduodamas į atitinkamą modulį išsiuntimui. Tad taikymo generuojami duomenys yra d = tbuf × f baitų, jei ignoruosime paketo papildomus bitus.

Song Jiaying ir Yen Kheng Tan straipsnyje [29] pateikta energijos sąnaudų ZigBee ir energijos kaupiklius naudojančiuose belaidžių jutiklių tinkluose analizė, atlikta siekiant praktiniu aspektu suprasti energijos poreikius energijos kaupimo technologijose. Analizuojamas trijų rūšių energijos suvartojimas, siekiant ištirti pagrindinius veiksnius, įtakojančius energijos kaupimo technologijų kūrimą: energijos suvartojimas galiniuose įtaisuose ir maršrutizatoriuose galios veiksena, energijos suvartojimas duomenų perdavimo metu naudojant mainų patvirtinimą ir be jo ir energijos suvartojimas maršrutizatoriuose, esant skirtingam mazgų tankiui. Remiantis atliktais matavimais, apibendrinti pagrindiniai rodikliai, lemiantys belaidžių jutiklių tinklų gyvenimo laiką, ir pasiūlytas energijos suvartojimo modelis, įvertinantis jutiklio mazgas gyvenimo laiką.

G.Kalic straipsnyje (Kalic, Goran, 2012) pateikia bevielių tinklų technologijų (Bluetooth, WiFi ir 3G) energijos suvartojimo matavimų rezultatus. Jų pagrindu pasiūlytas energijos suvartojimo modelis, įgalinantis paskaičiuoti energijos sąnaudas kiekvienai ryšių technologijai. Pademonstruotas šio modelio pritaikymas paslaugai, vadinamai kolektyviniu parsisiuntimu (angl. Collaborative Downloading). Pirminis šios paslaugos tikslas – sumažinti bendras mobiliųjų vartotojų

energijos sąnaudas, kai duomenys parsisiunčiami derinant kartu Bluetooth ir 3G arba WiFi ir 3G technologijas.

Modeliavimas gerai išvystytas mobiliesiems ir ad-hoc tinklams, pavyzdžiui, naudojant populiarų paketą ns2, tačiau besiskiriančios WSN charakteristikos ir našumo kriterijai įveda papildomus reikalavimus modeliavimui, o tai sąlygojo nemažo skaičiaus specialiai šiam tikslui skirtų modeliavimo priemonių ir jų išplėtimų atsiradimą. G.V.Merrett ir kt. straipsnyje [31] nagrinėja kelių žinomų modeliavimo priemonių tinkamumą mažomis energijos sąnaudomis pasižyminčių WSN įvertinimui ir siūlo naują struktūrą mažomis energijos sąnaudomis pasižyminčių WSN modeliavimui.

E.Casilari straipsnyje [23] pateikia baterijų energijos suvartojimo komerciniuose 802.15.4/ZigBee tinkluose empirinį įvertinimą. Šis įvertinimas remiasi iš maitinimo šaltinio tekančios srovės matavimu, vykdant skirtingas 802.15.4 ryšio operacijas. Matavimai sudaro galimybes apibrėžti analitinį modelį, skirtą mažiausio, vidutinio ir didžiausio baterijos tarnavimo laiko jutiklių tinkle prognozei, kaip jutiklio užimtumo ciklo ir surinktų duomenų dydžio funkcijai.

P.Park disertacijoje [24] pagrindinį dėmesį skiria valdymo taikymuose naudojamų WSN protokolų modeliavimo, analizės ir projektavimo karkasui pateikti. Protokolai suprojektuoti, siekiant minimizuoti energijos sąnaudas tinkle, atsižvelgiant į taikymo sluoksnio keliamus patikimumo ir delsos reikalavimus. Projektas remiasi protokolo elgesio analitiniu modeliavimu.

Lentelė 2.1 Modeliavimo programinės įrangos analizė

Modeliavimo programinė įranga	Modeliavimo tipas	Programavimo kalba	Grafinė vartotojo sąsaja/licenzija	Pastabos
GloMoSim	Lygiagretusis diskrečiųjų įvykių modeliavimas.	Parsec (programavimo kalba C pagrindu)	Yra Komercinė	Naudojant šią programą buvo testuojami keli WSN protokolų variantai.
JiST/SWANS	Diskrečiųjų įvykių modeliavimas.	Java baitinis kodas	Atviro kodo	JiST įrankio trūkumas, kad nepakankamas protokolų modelių skaičius. Programoje yra *ad-hoc* tinklo modeliavimo programa **SWANS**, turinti sumažintą protokolų palaikymą
J-Sim	Diskrečiųjų įvykių modeliavimas.	Java skriptų sąsaja (Perl, Tcl ir Phyton)	Yra Atviro kodo	J-Sim privalumas, kad palaiko nemažai protokolų.
NCTUns2.0	Diskrečiųjų įvykių modeliavimas.	UNIX mašinos branduolys	Nenurodyta	WSN modeliavimo modulių pridėjimas prie architektūros nėra paprastas uždavinys
NS-2	Diskrečiųjų įvykių modeliavimas.	Objektiškai orientuotas Tcl ir C++ išplėtimas	Nėra/ Atvirojo kodo	Apima WSN specifinių protokolų Directed Diffusion/SMAC Skurdus grafikos palaikymas, naudojant Nam.
OMNeT++	Diskrečiųjų įvykių modeliavimas.	C++ (Windows, Linux, MacOSX)	Yra Nekomercinė licencija,(OMNESET) komercinė licencija	OMNeT++ karkasas modeliavimo programoms kurti.

OPNET (nemokama akademiniams tyrimams)	Lygiagretusis diskrečiųjų įvykių modeliavimas.	C/C++, objektiškai orientuota	Yra Komercinė	Kiekvienam sistemos objektui apibrėžti naudojamas hierarchinis modelis. OPNET turi ESD (*External System Domain*) ryšiams su išorinėmis programomis ir sistemomis
Ptolemy II	Įvairūs modeliavimai	Java	Yra Atvirojo kodo	Skirtas lygiagrečiųjų, realaus laiko ir įterptinių sistemų modeliavimui, imitavimui ir projektavimui.
SSFNet	Diskrečiųjų įvykių modeliavimas	API JAVA ir C++	Yra Atviro kodo	Orientuota (lygiagrečiam) į labai didelės apimties ryšio tinklų modeliavimą
SWAN	Specifiniai išplėtimai, skirti *ad hoc* tinklams. Išplėsta, kad geriau vykdytų TinyOS kodą.			
TrueTime įrankiai (MATLAB)	Tinklinės ir įterptinės realaus laiko valdymo sistemos.	Matlab programavimas	Yra Atviro kodo	Palaiko *ZigBee* protokolą.

Žemiau lentelėje pateikti specifinių modeliavimo programų apibendrinti analizės duomenys.

Lentelė 2.2 Specifinės modeliavimo priemonės

Modeliavimo priemonės pavadinimas	**Grafinė vartotojo sąsaja**	**Licenzija**	**Programavimo ar operacinės sistemos**	**Pastabos**
ATEMU (AVR procesoriaus emuliatorius)	Yra. XTADB derinimo priemonė	Atviro kodo.	C (vykdoma TinyOS, ant MICA2 aparatinėje įrangoje)	Emuliuoja įvairius jutiklių mazgus homogeniniuose ir heterogeniniuose tinkluose didelių reikalavimų apdorojimui ir silpno plečiamumo sąskaita.
Avrora (AVR procesoriaus imitatorius) Jutiklių platforma Mica2 ir MicaZ.	Trūksta grafinės vartotojo sąsajos priemonių	Atviro kodo.	Java	Palaiko tūkstančių mazgų modeliavimą ir taupo vykdymo laiką.
COOJA/MSPSim (kodo lygio modeliavimo programinė įranga tinklams, kurie yra sudaryti iš Contiki OS dirbančių mazgų)	Nėra.	Nenurodyta	Java	Tame pačiame modeliavimo projekte galima naudoti mazgus su skirtinga modeliuojama technine įranga ir jų skirtinga programine įranga

EmCee	Sąsaja su realiais nedidelės galios radijo imtuvais, galinti generuoti radijo emuliaciją.			
EmSim	Mikroserverio aplinkos imitatorius; kiekvienas imituojamas mazgas vykdo Emtar steką ir yra prijungtas naudojant modeliuojamą radijo kanalo modelį.			
Emstar	Yra	Atviro kodo	C	Gali būti taikomas tik iPAQ klasės jutiklių mazgams ir MICA2 motes. .
Prowler/Jprowler	Yra	Specifnė	Vykdoma su Matlab/Java, skirta n/w parametrų optimizavimui. (matlab kodas)	Jprowler palaiko įstatomus radijo modelius ir MAC protokolus. Modeliuoja Berkley MICA motes.
Power Tossim	TinyOS imitatorius išplečia galios modelį į TOSSIM , įvertina kiekvieno mazgo energijos sąnaudas.			
Shawn	Nežinoma	Atvirojo kodo	Java	Adaptuojamas jutiklių tinklų imitatorius. Skirta labai didelių tinklų modeliavimui.
Tossf&Tython	Modeliavimo sistemos vykdo TinyOS taikomąsias programas, siekiant emuliuoti Berkely MICA mote hardware. TOSSF pagerina TOSSIM plečiamumą, Tython compliments TOSSIM executions prideda skriptų aplinką, kad papildytų modeliavimą			
Tossim	Yra	Atviro kodo.	TinyOS	Tossim korektiškai nemodeliuoja WSN energijos sąnaudų.
UWSim	Yra	Komercinė	C# Windows XP	Modeliuoja akustinį tinklą. Skirta povandeniniams jutiklių tinklams UWSN

Pagal lenteles galime matyti, kad modeliavimo priemonės neturi įrankių skirtų atlikti tyrimams energijos sąnaudų priklausomybės nuo apsaugos lygio ir aplinkos sąlygų.

2.1. Išvados

1. Nagrinėjamų modeliavimo priemonių pagrindinė paskirtis yra duomenų srautų ir maršrutizavimo protokolų tyrimai.
2. Negrinėtuose šaltiniuose nerasti modelių ar priemonių, kurios padėtų nustatyti komunikacinių protokolų energijos sąnaudų ir saugos priemonių modeliavimui ir tarpusavio ryšį.
3. Išnagrinėjus modeliavimo priemones, nerasta tinkama priemonė tirti energijos sąnaudų priklausomybę nuo saugos lygio ir aplinkos sąlygų. Todėl nuspręsta sudaryti hibridinį komunikacinį protokolo tyrimo modelį.

3. ZIGBEE PROTOKOLO EFEKTYVUMO TYRIMO HIBRIDINIS MODELIS

Modeliavimo tikslas ištirti daiktų interneto heterogeninių tinklų komunikacinių protokolų energetinių sąnaudų efektyvumą, atsižvelgiant į informacijos saugumą ir aplinkos sąlygas. Gautus rezultatus palyginti su kitų bevielių tinklų naudojamomis energijos sąnaudomis.

3.1. Hibridinis ZigBee protokolo tyrimo modeliai

Tiriamam belaidžio ryšio protokolui ZigBee sukuriamas hibridinis modelis. Hibridinis modelis sudarytas iš tokių dalių:

1. Prietaiso, realizuojančio belaidžio ryšio protokolus, aparatinis prototipas.
2. Programinė įranga, imituojanti įvairius protokolo darbo režimus.
3. Prototipo charakteristikų matavimo metodika
4. Matavimo rezultatų apdorojimo programinė įranga.

3.2. Prietaiso, realizuojančio belaidžio ryšio protokolus, prototipas

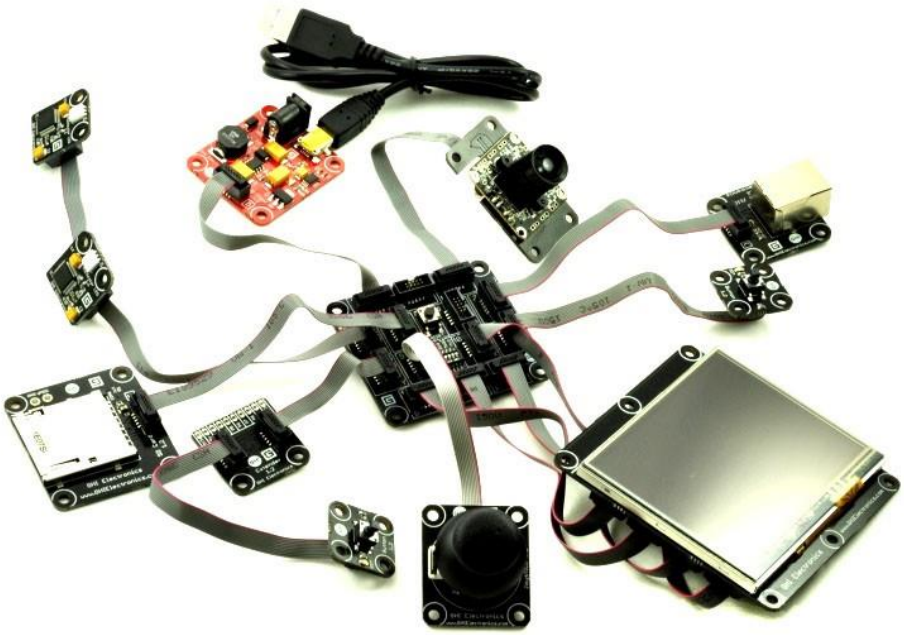
Prototipo realizacijai naudosime aparatinę platformą FEZ Spider Starter Kit, kuria sukūrė GHI electronics firma. Įrenginys, sukurtas naudojantis šia platforma, programuojamas Microsoft .NET Micro Framework.

.NET Gadgeteer (trumpiau Gadgeteer) yra Microsoft sukurta sistema, skirta mažiems elektronikos projektams kurti. Ji apjungia atvirojo kodo programinę įrangą (Apache 2.0 licencija) ir standartizuotą aparatinę platformą .NET Micro Framework (NETMF, taip pat Apache 2.0 licencija). Ši sistema sudaro galimybę labai greitai kurti prototipus, nesirūpinant sujungimų litavimu ar įvairių komutacinių laidų ir jungčių parinkimu. Toks Microsoft sumanymas, atitinkantis techninės ir programinės įrangos standartus, apibrėžia modulių sujungimo būdą ir formatus. Gadgeteer taip pat palaiko Visual Studio arba Visual C# Express integruotą kūrimo aplinką.

Modulius, atitinkančius Gadgeteer standartą, išleidžia keli gamintojai. Svarbiausias šios sistemos komponentas yra pagrindinė plokštė, kurioje yra 72MHz dažnio 32 bitų ARM7 procesorius, valdantis visus kitus komponentus, jungiamus prie pagrindinės plokštės.

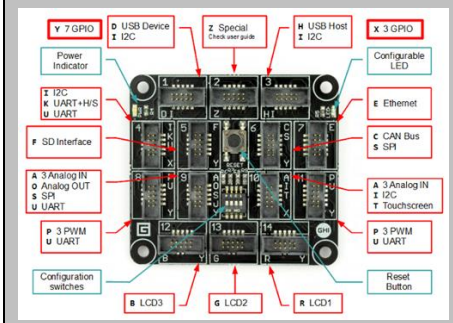
FEZ Spider komponentų rinkinys yra vienas iš populiaresnių Gadgeteer sistemų, kurioje yra viskas, ko reikia norint pradėti kurti nesudėtingus elektroninius įtaisus. Komplekte yra pagrindinė plokštė, kamera, daugiaspalviai šviesos diodai (LED), spalvotas jutiklinis ekranas ir įvairios kitos priemonės, taip pat ir reikalingos prisijungti prie kompiuterio ir interneto.

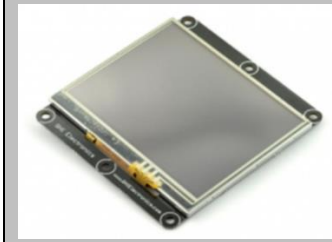
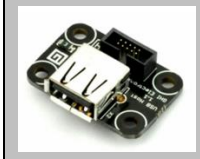
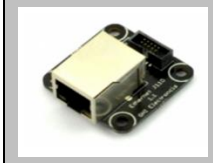
Fez Spider Starter Kit visi sujungti techninės įrangos elementai pateikti paveiksle žemiau:

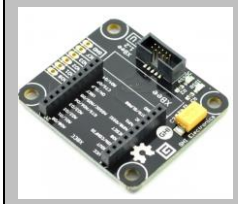


Pav. 3.1 FEZ Spider Starter Kit

Lentelė 3.1 FEZ Spider Starter Kit komponentai

Elementas	Aprašymas
Pagrindinė plokštė   	FEZ Spider pagrindinė plokštė yra suderinama su .NET Gadgeteer, sukurta GHI Electronics EMX modulio pagrindu. Šioje plokštėje realizuotos ne tik visos .NET Micro Framework branduolio savybės, tačiau ir kitos svarbios papildomos savybės, tokios kaip pagrindinis USB kontroleris (USB host), bevielis ryšys (WiFi) ir RLP (Radio Link Protocol – radijo ryšio protokolas, skirtas kodui įkrauti). Visos šios savybės leidžia greitai sukurti prototipą, naudojant GHI Electronics EMX modulį, kuriame yra: • 72MHz dažnio 32 bitų ARM7 procesorius; • 4.5 MB flash atmintis; • 16 MB RAM atmintis; • LCD kontroleris; • Pilna TCP/IP programinė įranga, realizuojanti SSL, HTTP, TCP, UDP, DHCP; • Ethernet, WiFi tvarkyklė ir PPP (GPRS/ 3G modemai) bei DPWS; • Pagrindinis USB kontroleris; • USB įtaisas su specializuotomis bibliotekomis, skirtomis tokiems įtaisams emuliuoti, kaip USB atmintukas, virtualus COM prievadas, pelė, klaviatūra; • 76 GPIO kontaktai; • 2 SPI (8/16 bitų); • I2C; • 4 UART; • 2 CAN kanalai;

	• 7 10 bitų analoginiai įėjimai; • 10 bitų analoginiai išėjimai (tinkami f WAV garso failams atkurti); • 4 bitų SD/MMC atminties plokštelės sąsaja; • 6 PWM; • OneWire sąsaja (esanti bet kuriame įvesties ir išvesties įtaise); • Įterptinis laikrodis (RTC - Real Time Clock) su atitinkamu kvarco kristalu; • Procesoriaus registrų prieiga; • OutputCompare aukšto tikslumo sinusoidės formos signalams generuoti; • RLP - radijo ryšio protokolas, kurį naudojant galima įkrauti kodą (C/Asemblerio) realaus laiko reikmėms; • Išplėsta dvigubo tikslumo skaičiavimų programinė įranga; • FAT failų sistema; • Kriptografijos (AES ir XTEA) priemonės; • Mažo energijos suvartojimo ir miego palaikymas; • Atnaujinimo priemonės (iš SD, kompiuterių tinklo ar kt.);
Prisilietimui jautrus ekranas T35 (320x240) 	320x240 3.5" spalvoto ekrano modulis su prisilietimui jautriu ekranu • Jungtys R,G,B LCD ekranui ir papildomas T skirta prisilietimui
Mygtukai (2 vnt.)  	Mygtukų modulis skirtas Gadgeteer tinkamiems įtaisams. Šis modulis turi konfigūruojamą LED šviesos diodą. • Lizdas: X arba Y
Pagrindinis USB kontroleris 	Naudodami pagrindinį USB kontrolerį, naudotojai gali perskaityti USB vairalazdės, pelės ir klaviatūros informaciją, taip pat gali įrašyti failus iš USB atminties kortelę ir perskaityti juos. GHI pagrindinis USB kontroleris palaiko šakotuvą. Prijungus šakotuvus, naudotojai gali prisijungti tiek USB įrenginių, kiek jie nori (iki 127 įrenginių - tokia yra USB sąsajos riba). Reikalingas H tipo lizdas ir USB kontrolerį palaikanti programinė įranga. • Lizdas: H
Ethernet modulis 	Šis Ethernet modulis Gadgeteer pagrindinei plokštei suteikia prieigą prie kompiuterių tinklo ir interneto. Ne visi Ethernet moduliai dirba kiekvienoje plokštėje, todėl reikia tai patikrinti. Šis modulis suderinamas su GHI FEZ Spider pagrindine plokšte. • Lizdas: E
Bluetooth Module	"Bluetooth" modulis leidžia Gadgeteer pagrindinei plokštei su belaidžiu ryšiu prisijungti prie kito "Bluetooth" prietaiso per SPP (Serial Port Profile), pavyzdžiui, prie mobiliųjų telefonų ir nešiojamų kompiuterių.

	
XBee PRO ZB ZigBee S2B Module  	Pagrindinės charakteristikos: • Protokolas pagrįstas IEEE 802.15.4 standartu, taigi užtikrina visas šiam protokolui būdingas charakteristikas ir funkcionalumą; • Palaiko skirtingas tinklo topologijas: įrenginys – įrenginys, žvaigždinę, medžio, tinklinis; • Maksimalus įrenginių skaičius tinkle iki 65535 (64 bitų IEEE adresavimo standartu); • Veikimas apie 50 metrų; • Veikia švyturėlio režimu. Tai leidžia įgyvendinti energiją taupančius koordinatorius ir maršrutizatorius; • Pasižymi energiją taupančiais maršrutizavimo algoritmais, duomenys persiunčiami geriausią signalo kokybę turinčiais maršrutizatoriais; • Naudoja 128 bitų AES duomenų kodavimo algoritmą; • Pasižymi mažais išteklių reikalavimais: ZigBee steko dydis apie 32 kB (sumažinto funkcionalumo įrenginiams apie 4 kB),
WiFi RS21 Module 	Savybės: • Suderinamas su 802.11b / g, 802.11n • Palaiko visas protokolų ir konfigūracijos funkcijas, reikalingas WLAN ryšiui atvirose ir WPA/WPA2-PSK saugiose veikimo režimuose. • Ypač mažos galios veikimas su energijos taupymo režimais • Ad-hoc ir infrastruktūros režimai • Ad hoc su WEP saugumo režimu.

Naudojantis **FEZ Spider Starter Kit** elementus sukonstruotas prototipas, kuris susideda iš pagrindinės plokštės, lietimui jautraus ekrano, belaidžio ryšio modulio ZigBee. Sukonstruotas įrenginys parodytas žemiau nuotraukoje:

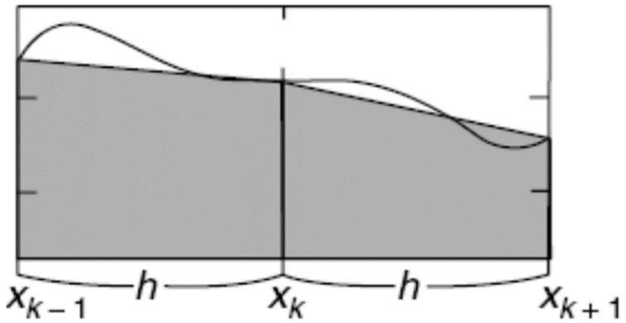
Pav. 3.2 Prototipas energijos sąnaudų matavimui

3.3. Modeliavimo programinė įranga

Šio prietaiso darbą ir režimus imituoja programinė įranga, parašyta su mikro .NET karkasu.

Eksperimento metu gauti rezultatai apdoroti MATLAB programinės įrangos pagalba.

Tyrime pasirinkta skaičiuoti pasitelkus skaitinį integravimą. Skaitinio integravimo pagalba randamas galios vartojimo kreivės plotas, kuris atitinkamas atliktam darbui. Iš esamų skaitinių integravimo metodų, pasirinktas trapecinis skaitinis integravimas. Šiame metode plotas, po kreive, skaidomas į atitinkamą kiekį intervalų, kiekviename jų yra skaičiuojamas trapecijos plotas. Kiekvienas intervalas bandomas kuo labiau pritaikyti prie kreivės formos. Paveiksle žemiau parodytas skaidymas į trapecijas:



Pav. 3.3. Ploto po kreive, skaidymas į trapecijas.

Trapecijos plotas apskaičiuojamas pagal sekančią formulę:

$$\int_{x_k}^{x_{k+1}} f(x)dx;$$

Visas plotas, esantis po kreive bus apskaičiuojamas:

$$\sum_{k=0}^{n-1} \int_{x_k}^{x_{k+1}} f(x)dx$$

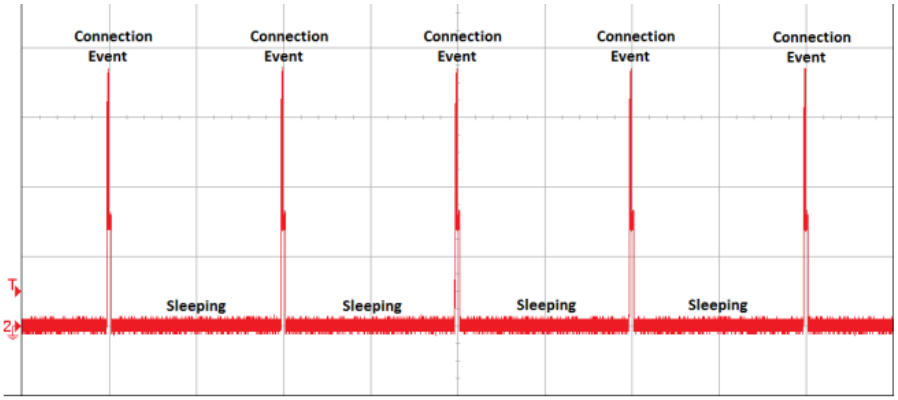
Gautų duomenų apdorojimui naudojama MATLAB programinė įranga, kurioje yra realizuotas trapecijų skaitinis integravimo metodas. Programoje ši funkcija yra pavadinta *trapz*, kurios pagalba buvo atlikti aukščiau aprašyti skaičiavimai.

3.4. Prototipo charakteristikų matavimo metodika

Tiriamo modelio charakteristikų matavimo metodika parengta pagal Texas Instrumens metodika[3].

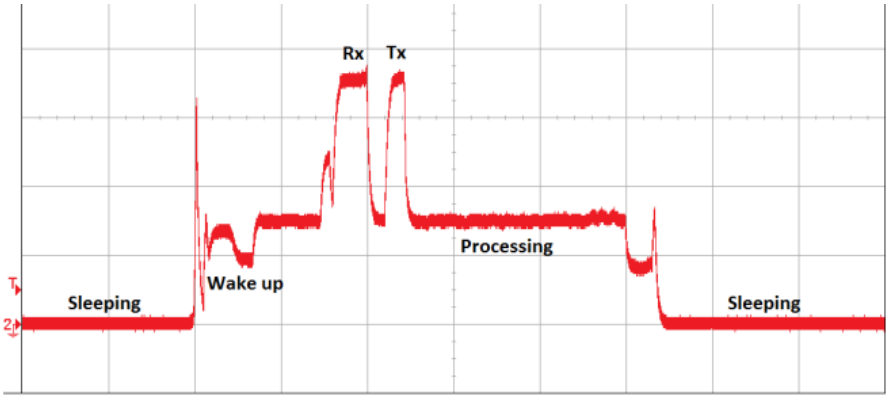
Ryšio prietaiso energijos sąnaudų neįmanoma įvertinti, naudojant tik vieną matavimo vienetą. Prietaisų gamintojai dažniausiai nurodo įrenginio maksimalią naudojamą galią. Nors ši galia yra svarbus rodiklis bendram energijos suvartojimui, bet ryšio prietaisas maksimalią galią naudoja tik kai vyksta duomenų perdavimas. Net ir labai didelio našumo sistemose, ryšio įrenginiai informaciją perduoda tik nedidelę savo darbo laiko dalį.

[3] http://www.ti.com/lit/an/swra177/swra177.pdf



Pav. 3.4. Ryšio įrenginio energijos suvartojimas laike[1].

Įvairūs ryšio įrenginiai dirba skirtingose būsenose: budėjimo būsena (kai įrenginys naudoja minimaliai energijos), aktyvavimosi būsena (energijos sąnaudos staiga pradeda didėti), duomenų perdavimo būsena (dažniausiai energijos sąnaudos naudojamos maksimaliai), duomenų apdorojimo būsena ir įrenginio deaktyvavimosi būsena, perėjimas į budėjimo būseną (pav. 3.5). Net jei prietaiso galia visose būsenoje yra žinoma, tai nėra pakankamai informacijos, kad būtų galima nustatyti visas energijos sąnaudas. Skirtinguose komunikavimo protokolo sluoksniuose, bei režimuose atliekamas skirtingas duomenų apdorojimas, kuris reikalauja skirtingų energijos sąnaudų. Į visa tai turi būti atsižvelgta, siekiant gauti tikslų energijos sąnaudų įvertinimą.



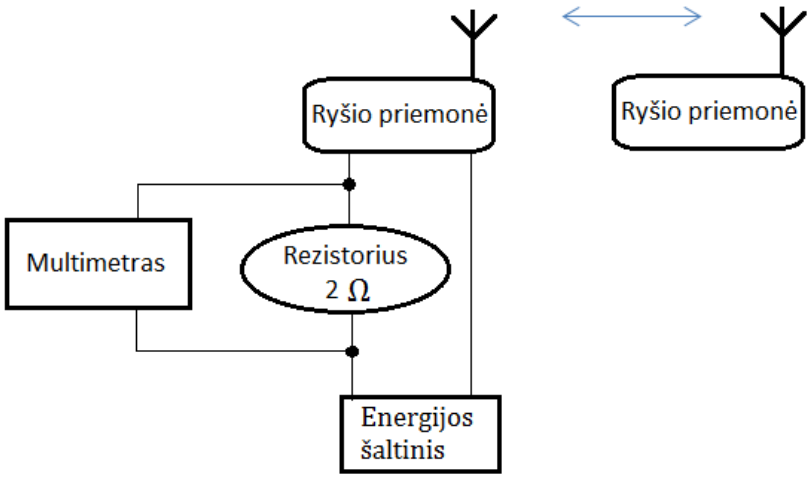
Pav. 3.5. Ryšio įrenginio energijos suvartojimo kitimas skirtingose būsenose[1].

Dažniausiai prietaisas didžiausią laiko dalį būna budėjimo režimu, saugomas prietaiso registrų ir atminties turinys. Prietaisas gavęs pertraukties signalą aktyvuojasi, atlikti duomenų perdavimo ir apdorojimo operacijas.

Pagrindinis rodiklis, kuris gali būti naudojamas, nust atant prietaiso baterijos gyvavimą, yra vidutinė prietaiso naudojama galia tam tikro taikymo atveju. Tačiau viena "vidutinės galios" vertė negali būti nurodoma prietaiso specifikacijoje, nes vidutinė galia labai priklauso nuo ryšio parametrų, bei aplinkos sąlygų (eterio radijo „užterštumas“ ir t.t.). Įrenginio aprašyme nurodoma vidutinė galia, tačiau nežinome sąlygų kokiomis ji buvo išmatuota ar kokios gali būti prietaiso konkretaus taikymo sąlygos.

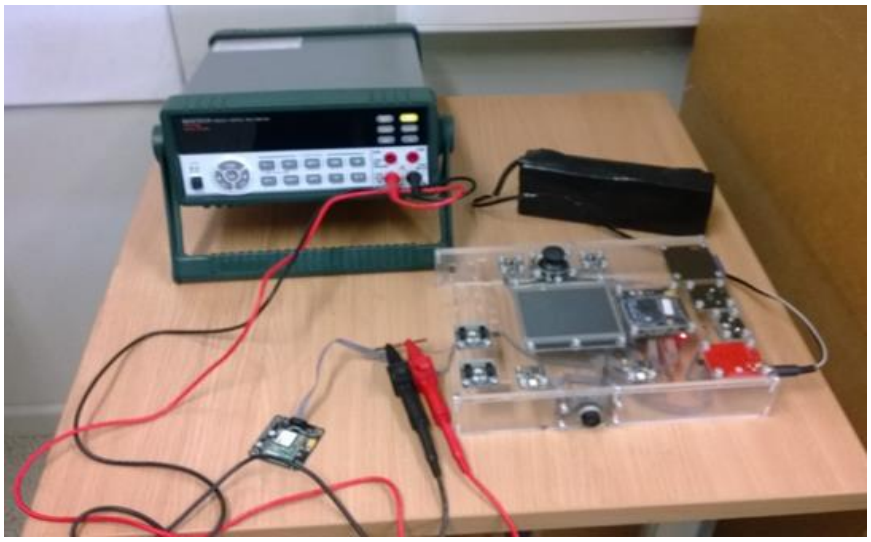
Prietaiso naudojamą elektros srovę matuosime skirtingose prietaiso būsenose. Siekiant tinkamai nustatyti vidutinį energijos sąnaudas, tokie matavimai bus atliekami laike. Kadangi ryšio prietaiso būsenos dažniausiai labai greitai kinta laike (ms trukmės), todėl matavimai turėtų būti atlikti su oscilografu. Tačiau mus domina visos energijos sąnaudos darbo metu, neišskiriant prietaiso įvairių būsenų, mes naudosime skaitmeninį multimetrą, kuris matuoja srovę/įtampą 0,5 s intervalais. Paprasčiausias būdas matuoti srovę yra naudoti specialų zondą. Tačiau mes naudojamą srovę apskaičiuosime išmatavę įtampą ant rezistoriaus įjungto į prietaiso maitinimo grandinę. Bus

naudojamas 2 Ω rezistorius, nes tokia vertė yra pakankamai maža, kad nebūtų įtakos schemai, ir pakankamai didelė, kad būtų įtampos kritimas, kuris bus išmatuotas geru tikslumu. Matavimo stendo schema žemiau:



Pav. 3.3 Matavimo stendo schema

Matavimo įranga paruošta darbui pavaizduota žemiau paveiksle:



Pav. 3.4 Matavimo įranga

Tyrimui atlikti naudojami dviejų tipų XBee moduliai XBee S2 ir XBee PRO S2B. Šie moduliai pavaizduoti paveiksle žemiau, bei pateikta specifikacijų lentelė.

Pav. 3.5 XBee S2 ir XBee PRO S2B

XBee modulių specifikacijos pateiktos žemiau lentelėje. Nurodyti svarbiausi parametrai šiame darbe.

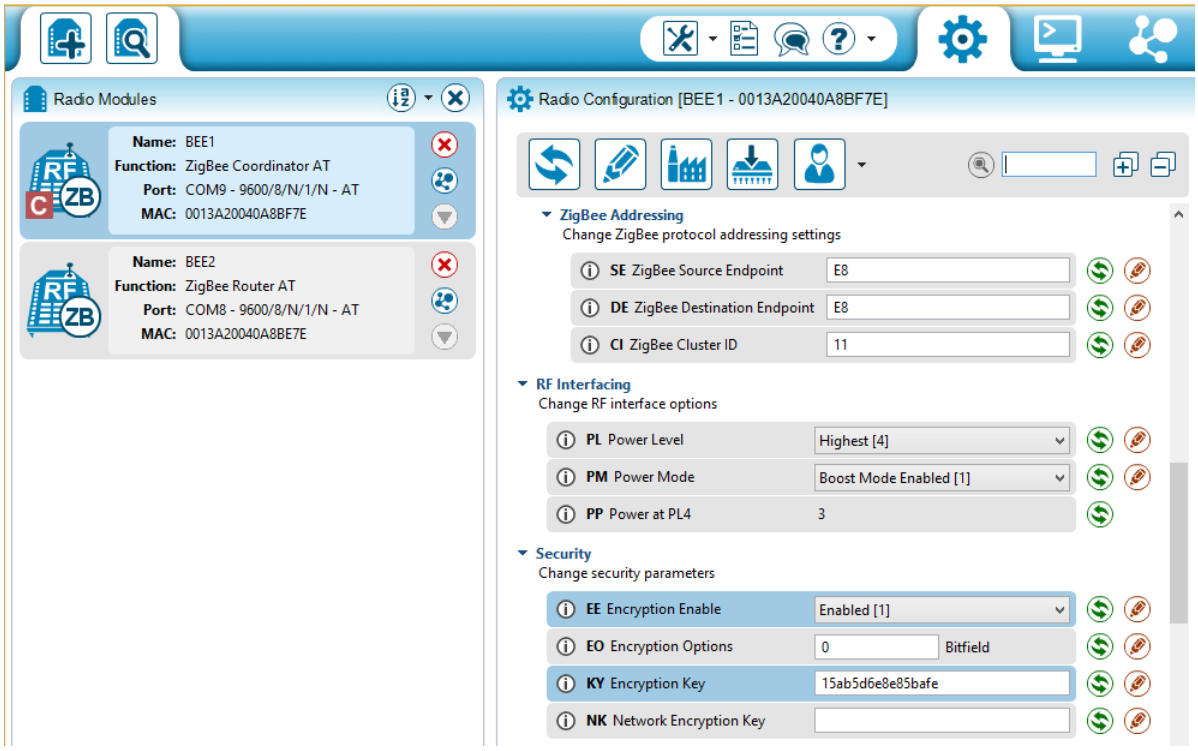
Lentelė 3.2 XBee S2 ir XBee PRO S2B specifikacijų palyginimas

	XBee S2	**XBee PRO S2B**
Duomenų perdavimo greitis	250 Kbps	
Ryšio nuotolis patalpose	40 m	90 m
Ryšio nuotolis lauke, tiesioginėmis matymo sąlygomis	120 m	1500 m
Imtuvo jautrumas	-96 dBm	-102 dBm
Dažnių juosta	2.4 GHz	
Darbinė temperatūra ir drėgmė	Nuo -40 ° C iki + 85 ° C, 0-95% drėgmės kondensacija	
Šifravimas	128-bitų AES	
Patikimas paketų pristatymas	Pakartojimai/padėka	

Xbee moduliai konfigūruojami per jiems skirtą adapterį, kuris jungiasi per USB prievadą.

Pav. 3.6 XBee adapteris

Xbee modulių konfigūravimui naudojama XCTU nemokama programa, kuri leidžia kūrėjams bendrauti su radijo moduliais per paprastą grafinę sąsają. Pagrindinės XCTU funkcijos yra valdyti ir konfigūruoti XBee prietaisus, net ir nuotoliniu būdu, mikroprogramos (angl. firmware) atnaujinimas, unikali funkcija atvaizduoti grafinį tinklą, kuris parodo kiekvieno įrenginio jungties stiprumą.



Pav. 3.7 XCTU programa

Per XCTU programa konfigūruojasi XBee modulio saugos parametrai. Šifravimas gali būti įjungtas arba išjungtas, taip pat galima įvesti norimą šifravimo raktą.

Programos duomenims siųsti ir gauti parašytos su C# programavimo kalba, naudojant Microsoft Visual Studio 2013 programinės įrangos kūrimo platformą.

Programa siunčia 100 KB duomenų, kai šis kiekis išsiunčiamas, sistema baigia darbą.

```
public class Program
    {
        public static void Main()
        {
          Debug.Print("Programa siuncia informacija(XBee)");
          int duomenuKiekis = 0;
          xBeeAdapter.Configure(9600,
GT.Interfaces.Serial.SerialParity.None,
GT.Interfaces.Serial.SerialStopBits.One, 8);
            xBeeAdapter.SerialLine.Open();
            string tekstas = "Labas.";
            byte[] duomenys = new byte[128];
            duomenys = Encoding.UTF8.GetBytes(tekstas);
            while (duomenuKiekis < 102400)
            {
                duomenuKiekis += duomenys.Length;
                xBeeAdapter.SerialLine.Write(duomenys);
            }
        }
    }
```

Programa priima siunčiamus duomenis. Kai įrenginys gauna 100 KB duomenų, darbas sustabdomas.

```
public class Program
    {
        void ProgramStarted()
        {
            Debug.Print("Programa gauna XBee duomenis");
            int duomenuKiekis = 0;
            xBeeAdapter.Configure(9600,
GT.Interfaces.Serial.SerialParity.None,
GT.Interfaces.Serial.SerialStopBits.One, 8);
            xBeeAdapter.SerialLine.Open();
            byte[] duomenys = new byte[128];
            while (duomenuKiekis < 102400)
            {
             xBeeAdapter.SerialLine.Read(duomenys, 0, duomenys.Length);
             duomenuKiekis += duomenys.Length;
             Debug.Print("Gauti duomenys: " + duomenys);
            }
          }
     }
```

3.5. Išvados

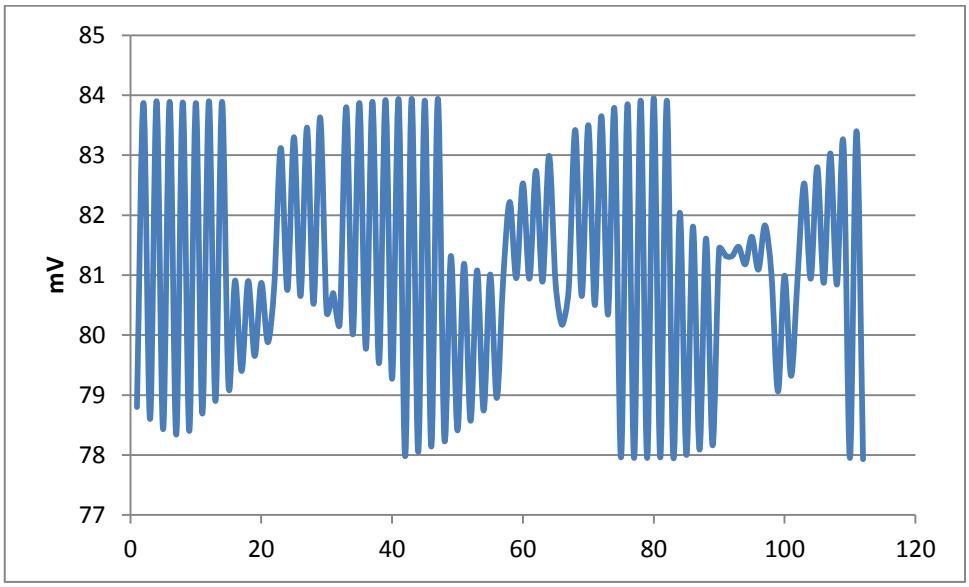
ZigBee protokolo modelį sudaro FEZ Spider Starter Kit, du XBee S2 ir du XBee PRO S2B. Energijos suvartojimas matuojamas naudojant pora XBee S2 modulių, o po to jie pakeičiami į XBee PRO S2B. Vienas XBee modulis jungiamas į FEZ Spider įrenginį, kitas į kompiuterį. Matuojama energija kai informacija siunčiama iš FEZ Spider įrenginio per XBee modulį ir kai informacija gaunama iš kompiuterio į FEZ Spider įrenginį per XBee modulį.

4. ZIGBEE PROTOKOLO ENERGIJOS SĄNAUDŲ TYRIMAS

Siuntimui naudojamas 128 baitų buferis, siunčiama 100 KB informacijos. Eksperimentas atliekas realiose sąlygose, randama apie 10 WiFi prieigos taškų.

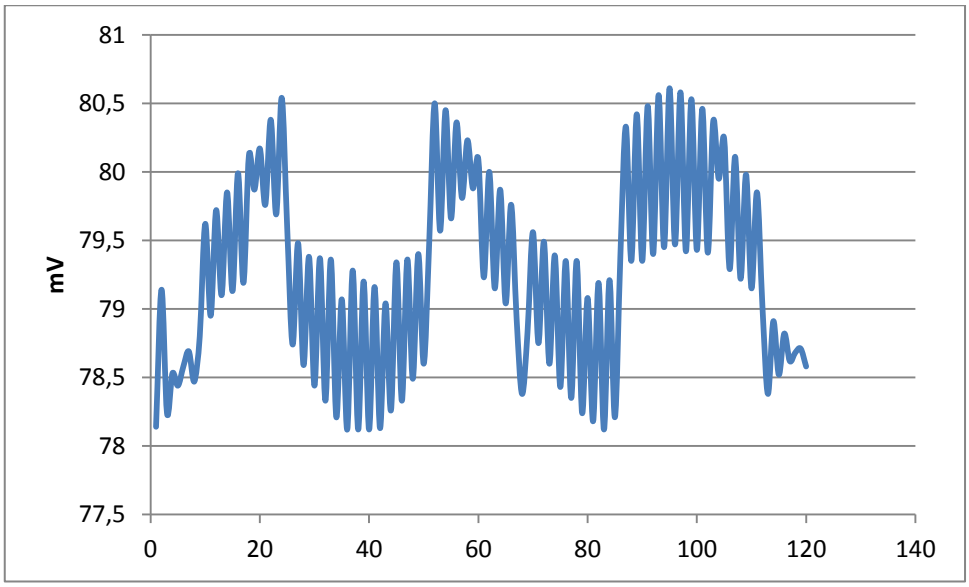
XBee S2 modulis

Vidutinė XBee S2 koordinatoriaus modulio naudojama įtampa: 81,07 mV



Pav. 4.1 XBee S2 koordinatoriaus įtampa

Vidutinė XBee S2 maršrutizatoriaus modulio naudojama įtampa: 79,27 mV



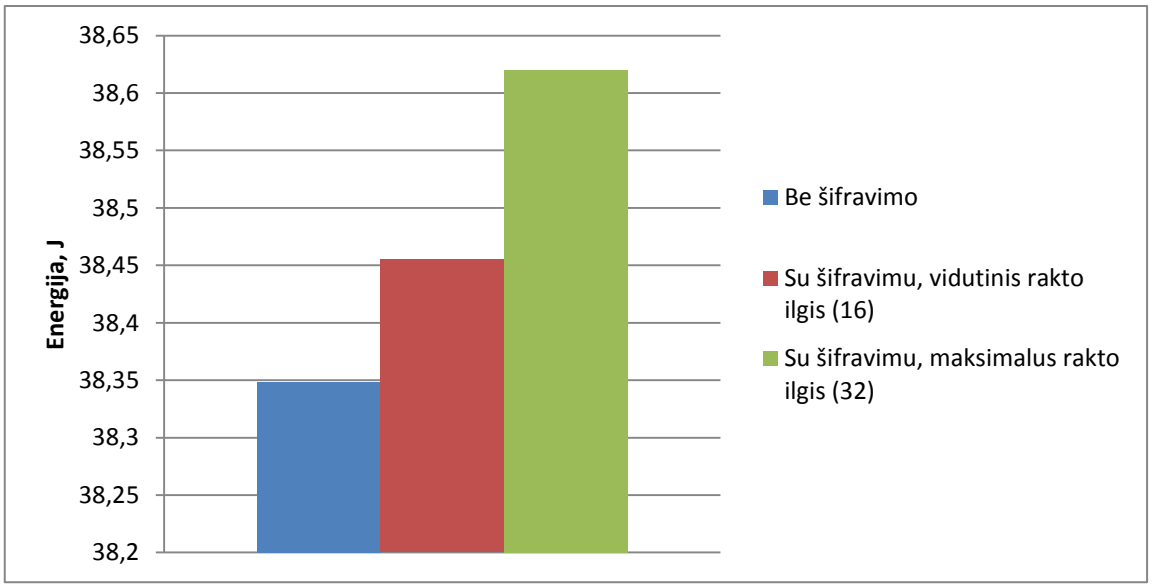
Pav. 4.2 XBee S2 maršrutizatoriaus įtampa

Šifravimui naudojami raktai:
Vidutinis raktas: a5b7d899eb6f5893
Maksimalaus ilgio raktas: a5b7d899eb6f5893a2d0b3c66ddf6e5d

Žemiau pateikiamas energijos sąnaudų palyginimo grafikas, naudojant XBee S2. Pirmame stulpelyje pavaizduota kai duomenys siunčiami nešifruoti. Antrame stulpelyje pavaizduotas duomenų siuntimas su vidutinio ilgio raktu, o trečiame duomenų siuntimas su maksimaliu šifravimo rakto ilgiu.

Lentelė 4.1 XBee S2 duomenų perdavimo laiko palyginimas

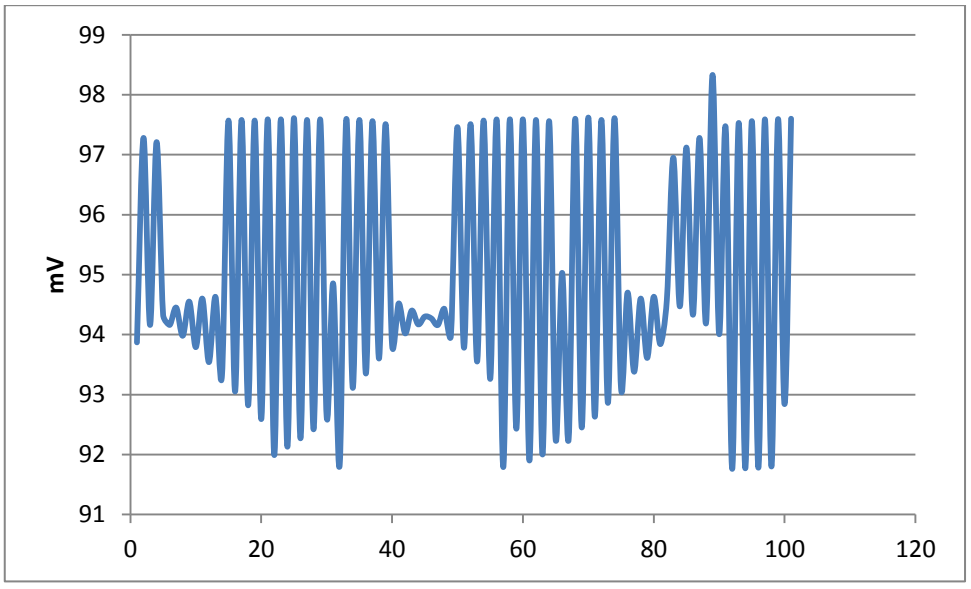
Be šifravimo	Su šifravimu, vidutinis rakto ilgis (16)	Su šifravimu, maksimalus rakto ilgis (32)
01:53	01:58	02:02



Pav. 4.3 XBee S2 energijos suvartojimas siunčiant duomenis

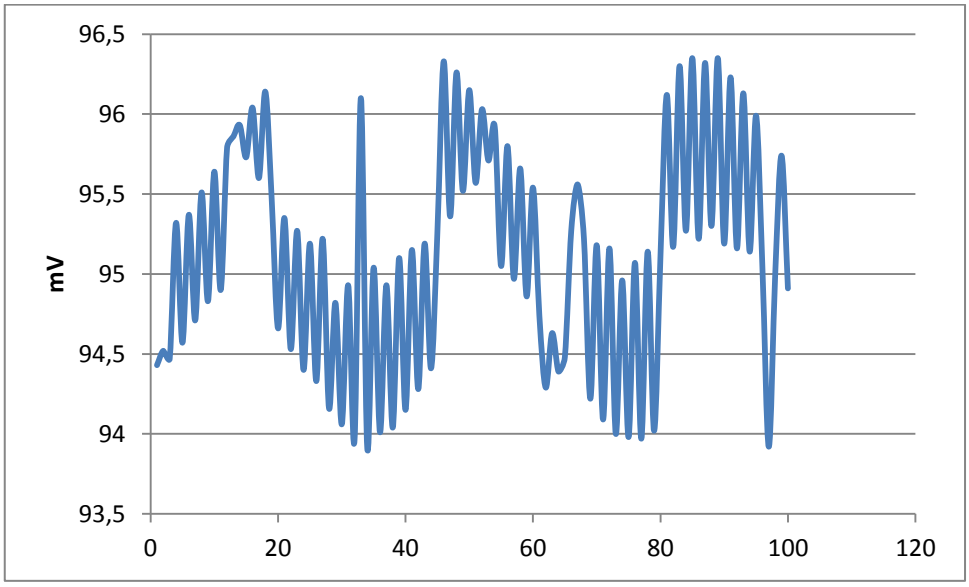
XBee PRO S2B modulis

Vidutinė XBee PRO S2B koordinatoriaus modulio naudojama įtampa: 94,90 mV



Pav. 4.4 XBee PRO S2B koordinatoriaus įtampa

Vidutinė XBee PRO S2B maršrutizatoriaus modulio naudojama įtampa: 95,12 mV

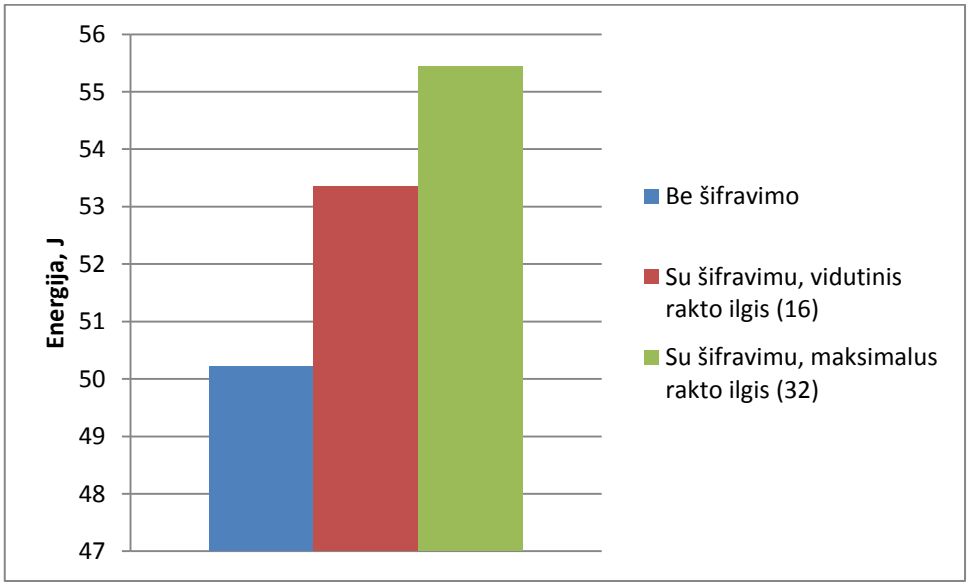


Pav. 4.5 XBee PRO S2B maršrutizatoriaus įtampa

Žemiau pateikiamas energijos sąnaudų palyginimo grafikas, naudojant XBee PRO S2B. Pirmame stulpelyje pavaizduota kai duomenys siunčiami nešifruojami. Antrame stulpelyje pavaizduotas duomenų siuntimas su vidutinio ilgio raktu, o trečiame duomenų siuntimas su maksimaliu šifravimo rakto ilgiu.

Lentelė 4.2 XBee PRO S2B duomenų perdavimo laiko palyginimas

Be šifravimo	Su šifravimu, vidutinis rakto ilgis (16)	Su šifravimu, maksimalus rakto ilgis (32)
01:52	01:57	02:01



Pav. 4.6 XBee PRO S2B energijos suvartojimas siunčiant duomenis

XBee modulių energijos suvartojimo palyginimas XBee S2 ir XBee PRO S2B

4.1. Išvados

1. Atlikus tyrimą nustatytas ZigBee modulių energijos suvartojimas siunčiant duomenis. Duomenų siuntimas suvartojo daugiau energijos kai buvo ilgesnis šifravimo raktas.
2. ZigBee modulyje įjungus šifravimą AES 128 bitų, energijos suvartojimas padidėjo apie 10%.
3. Reali duomenų perdavimo sparta buvo vidutiniškai 1,17 KB/s.
4. Lyginant XBee S2 ir XBee PRO S2B modulius, naudojant nedidelį atstumą nustatyta, kad greitaveika beveik nesiskiria.

5. IŠVADOS

Darbo metu atlikta analizė daiktų interneto protokolų saugos lygio, energijos sąnaudų tarpusavio ryšio ir priklausomybės nuo aplinkos sąlygų. Išanalizuoti populiarūs daiktų interneto protokolai. Ištirta ZigBee protokolo energijos suvartojimas naudojant ir nenaudojant šifravimo.

Išnagrinėtose komunikacinių protokolų modeliavimo priemonėse pagrindinė paskirtis yra duomenų srautų ir maršrutizavimo protokolų tyrimai, tačiau nerasta modelių ar priemonių, kurios padėtų nustatyti komunikacinių protokolų energijos sąnaudų ir saugos priemonių modeliavimui ir tarpusavio ryšį.

Sudarytas eksperimentinis modelis, kurio pagalba buvo atliktas energijos suvartojimo tyrimas. Pagal atliktą tyrimą matome, kad ZigBee komunikaciniame protokole duomenų šifravimas daro įtaką energijos suvartojimui, siunčiant šifruotis duomenis siuntimas užtruko ilgiau.

Idealioje aplinkoje – tokioje vietoje kur nėra papildomų radijo bangas skleidžiančių įrenginių, duomenų siuntimas turėtų būti efektyvesnis.

Atlikus tyrimą nustatytas ZigBee modulių energijos suvartojimas siunčiant duomenis. Duomenų siuntimas suvartojo daugiau energijos kai buvo ilgesnis šifravimo raktas.

ZigBee modulyje įjungus šifravimą AES 128 bitų, energijos suvartojimas padidėjo apie 10%.

Reali duomenų perdavimo sparta buvo vidutiniškai 9,36 Kb/s, o gamintojas nurodo teorinę 250 Kb/s.

Lyginant XBee S2 ir XBee PRO S2B modulius, naudojant nedidelį atstumą nustatyta, kad greitaveika beveik nesiskiria.

Nustatyta, kad ZigBee bevielio ryšio tinklas tinka ten kur nereikalauja didelės duomenų perdavimo spartos. Toks tinklas gali būti saugus, o baterijos, kurios maitina mazgus, ilgai veikia, nes vienas iš svarbiausių ZigBee tinklų prioritetų yra energijos taupymas.

Apibendrinimui galima teigti, kad ZigBee protokolas tinkamas pasirinkimas daiktų internetui, kadangi naudoja mažai energijos, be to tinkle gali būti iki 65535 įrenginių.

Sparčiai plėtojantis daiktų internetui, ateityje didės problema dėl energijos suvartojimo, bus reikalingi dar mažiau energijos suvartojantys duomenų perdavimo ir saugos protokolai. Taip pat didės saugumo problemos,

LITERATŪRA

[1] Chen l, Ji J, Zhang Z (editors) (2012). Wireless Network Security: Theory and Applications.

[2] Measuring the Power Consumption on eZ430-RF2480, žiūrėta [2015-05-04]. Prieiga per internetą: http://www.ti.com/lit/an/swra177/swra177.pdf

[3] ZigBee Technology, žiūrėta [2015-05-04]. Prieiga per internetą: http://www.zigbee.org

[4] [Labiod, et al., 2007] Labiod, H.,H. Afifi, C. De Santis (2007). WI-FI, BLUETOOTH, ZIG BEE AND WIMAX. Dordrecht, The Netherlands.

[5] Saugaus maršrutizavimo Ad Hoc tinkluose tyrimas (2011) , žiūrėta [2015-05-06]. Prieiga per internetą: http://vddb.laba.lt/fedora/get/LT-eLABa-0001:E.02~2011~D_20110831_112815-19717/DS.005.0.01.ETD .

[6] Meng JT, Feng SZ et al. , Yuan JR (2013). An energy efficient clustering scheme for data aggregation in wireless sensor networks. Journal of computer science and technology.

[7] ZigBee, žiūrėta [2015-05-05]. Prieiga per internetą: http://www.libelium.com/security-802-15-4-zigbee

[8] Kamel, M., K. Boudaoud, S. Lequeux, and M. Riveill (2010). "Designing Security Protocols Adapted to the Constraints of Mobile Environments", Embedded and Ubiquitous Computing (EUC), IEEE/IFIP 8th International Conference, vol., no., pp.624–629, 11–13 Dec. 2010.

[9] Prasithsangaree, P. and P. Krishnamurthy (2004). "On a framework for energy-efficient security protocols in wireless networks", Computer Communications, vol. 27, is. 17, pp. 1716–1729, Nov.

[10] A. V. Taddeo ir A. Ferrante - „Run-time Selection of Security Algorithms For Networked Devices" 2009.

[11] Cano, M. D. and G. Domenech-Asensi (2011). "A secure energy-efficient m-banking application for mobile devices", Journal of Systems and Software, vol. 84, is. 11, pp. 1899–1909.

[12] Potlapally, N.R., S. Ravi, A. Raghunathan, R.B. Lee, and N.K. Jha, (2007). "Configuration and Extension of Embedded Processors to Optimize IPSec Protocol Execution", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 15 (5), pp. 605–609.

[13] [Venčkauskas et al., 2012A] Venčkauskas, A., N. Jusas, I. Mikuckienė, S. Maciulevičius (2012A). "Generation of the secret enc-ryption key using the signature of the embedded system", Information technology and control, T. 41, nr. 4, pp. 368–375.

[14] [Venčkauskas et al., 2012] Venčkauskas, A., N. Jusas, L. Kižauskienė, E. Kazanavičius, and V. Kazanavičius (2012). "Security method of embedded software for mechatronic systems", Mechanika, T. 18, nr. 2, pp. 196–202.

[15] .NET Micro Framework (NETMF) , žiūrėta [2015-05-10]. Prieiga per internetą: https://netmf.codeplex.com

[16] .NET Gadgeteer , žiūrėta [2015-05-04]. Prieiga per internetą: http://www.netmf.com/gadgeteer

[17] FEZ Spider Starter Kit, žiūrėta [2015-05-04]. Prieiga per internetą: https://www.ghielectronics.com/catalog/product/297

[18] Weber, R. H. (2010). "Internet of Things – New security and privacy challenges", Computer Law & Security Review, vol. 26, 1, pp. 23–30.

[19] Jara A. J., D. Fernandez, P. Lopez, M. A. Zamora, L.Marin and A. F. Skarmeta (2013). Evaluation of Bluetooth Low Energy Capabilities for Tele-mobile Monitoring in Home-care. Journal of Universal Computer Science, vol. 19, no. 9, pp. 1219-1241.

[20] Freier, A., P. Karlton, and P. Kocher (2011). "The Secure Sockets Layer (SSL) Protocol Version 3.0".

[21] [Toldinas , 2011] Toldinas, J., V. Stuikys, R. Damasevicius, G. Ziberkas, and M. Banionis (2011). "Energy efficiency comparison with cipher strength of AES and Rijndael cryptographic algorithms in mobile devices", Electronics and Electrical Engineering, 2(108), pp. 11–14.

[22] Kansal, A., F. Zhao, J. Liu, N. Kothari, and A. A. Bhattacharya (2010). "Virtual machine power metering and provisioning", In Proceedings of the 1st ACM symposium on Cloud computing

(SoCC '10), ACM, New York, NY, USA, pp. 39–50.
[23] Casilari, E., Cano-García, J. M., & Campos-Garrido, G. (2010). Modeling of current consumption in 802.15. 4/ZigBee sensor motes. Sensors, 10(6), 5443-5468.
[24] PARK, Pangun. Modeling, Analysis and Design of Wireless Sensor Network Protocols. 2011. PhD Thesis. KTH.
[25] Hongwei Li ; Zhongning Jia ; Xiaofeng Xue . Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on Volume: 2, Page(s): 494 - 497
[26] Jin-Shyan Lee, Yu-Wei Su, Chung-Chou Shen, (2007). A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. Industrial Electronics Society, IECON 2007. 33rd Annual Conference of the IEEE, vol., No., 46-51.
[27] Tozlu, Serbulent, and Murat Senel. "Battery lifetime performance of Wi-Fi enabled sensors." Consumer Communi-cations and Networking Conference (CCNC), 2012 IEEE. IEEE, 2012.
[28] Malavenda, Claudio S., Francesco Menichelli, and Mauro Olivieri. "Delay-Tolerant, Low-Power Protocols for Large Security-Critical Wireless Sensor Networks." Journal of Computer Networks and Communications 2012 (2012).
[29] Song, Jiaying, and Yen Kheng Tan. "Energy consumption analysis of ZigBee-based energy harvesting wireless sen-sor networks." Communication Systems (ICCS), 2012 IEEE International Conference on. IEEE, 2012.
[30] Kalic, Goran, Iva Bojic, and Mario Kusek. "Energy consumption in android phones when using wireless communi-cation technologies." MIPRO, 2012 Proceedings of the 35th International Convention. IEEE, 2012.
[31] Merrett, Geoff V., et al. "Energy-aware simulation for wireless sensor networks." Sensor, Mesh and Ad Hoc Com-munications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on. IEEE, 2009.
[32] Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments, žiūrėta [2015-05-07]. Prieiga per internetą: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf
[33] Karunakar Pothuganti and Anusha Chitneni, A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi, žiūrėta [2015-05-09]. Prieiga per internetą: http://www.ripublication.com/aeee_spl/aeeev4n6spl_18.pdf