KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Inga Gudaitytė

Delninukų bevielio ryšio saugos protokolų tyrimas

Magistro darbas

Darbo vadovas
Doc. dr. J. Toldinas

Kaunas, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Inga Gudaitytė

Delninukų bevielio ryšio saugos protokolų tyrimas

Magistro darbas

Recenzentas
lekt. dr. A. Liutkevičius
2011-05-

Vadovas
doc. dr. J. Toldinas
2011-05-27

Atliko
IFN-9/3 gr. stud.
Inga Gudaitytė
2011-05-27

Kaunas, 2011

Turinys

ĮVADAS

Visų elektroninių prietaisų naudojimas paremtas energijos vartojimu. Ne išimtis nešiojami kompiuteriai, mobilieji bei sumanieji telefonai, kurie naudoja pakraunamas baterijas. Baterijų veikimo laikas yra trumpas, todėl šie prietaisai linkę labai greitai išsikrauti. Kadangi šios technologijos yra populiarios, jose įdiegiama vis daugiau funkcijų, kurių naudojimas tik paspartina baterijos išsikrovimą.

Delniniai kompiuteriai yra naudojamasi komunikacijai su kitais kompiuteriais bei prieigai prie interneto resursų, todėl yra svarbu užtikrinti norimos persiųsti informacijos saugumą. Šiai funkcijai užtikrinti naudojami saugos protokolai. Bevielė tinklo infrastruktūra remiasi tokiomis kaip „Wi-Fi“, „Bluetooth“, „WiMax“ technologijomis. Mūsų dėmesys skirtas Wi-Fi technologijai, nes jos palaikymas įdiegtas visose populiariausiose operacinėse sistemose, ji komplektuojama daugelyje šiuolaikinių nešiojamų bei delninių kompiuterių. Magistrinio darbo tyrimo sritis yra informacijos sauga, naudojant bevielio interneto prieigą – Wi-Fi, ir kokią įtaką ji turi energijos suvartojimui. Darbo objektas – mobilieji įrenginiai su baterija: išmanieji telefonai, delninukai ir kt. Tyrimo tikslas – sudaryti matavimo metodiką, kurios pagalba galima įvertinti energijos suvartojimą priklausomai nuo pasirinkto Wi-Fi saugos protokolo delninukuose. Juos ištyrus bus galima patarti naudotojams kokį saugos protokolą pasirinkti priklausomai nuo jų naudojamų funkcijų delniniame kompiuteryje, bei pasiūlyti sprendimą mažesniam energijos suvartojimui. Tyrimui įgyvendinti naudojamas delninis kompiuteris, veikiantis Windows Mobile aplinkoje.

Tyrimai, susiję su mobiliais įrenginiais, yra atliekami ne tik užsienio mokslininkų. J. Toldinas, V.Štuikys, R.Damaševičius ir G. Ziberkas 2009 metais atliko tyrimą, kuriame išnagrinėti mobiliųjų įtaisų energijos naudojimo taikomojo lygmens modeliai, kurie turi įtakos energijos naudojimui bevieliam ryšiui Wi-Fi [18]. 2010 metais žurnale „Elektronika ir elektrotechnika“ pasirodė straipsnis „Energijos suvartojimo kriptografijos paslaugos algoritmams eksperimentas“, kuriame nagrinėjama energijos vartojimo supratimo ir informacijos apsaugos mobiliuosiuose įtaisuose problema [19]. Straipsnyje pateikiami eksperimento su keturiais kriptografiniais algoritmais (DES, 3DES, AES, RC2) rezultatai, siekiant nustatyti jų energijos imlumą, bei surinkti duomenis, kad būtų galima rasti įvairių charakteristikų tarpusavio priklausomybes.

Darbo struktūra:

Darbo analizės dalyje aptariama darbo problema. Surasti ir aprašyti egzistuojantys bevielių tinklų energijos taupymo sprendimai ir sąnaudas mažinantys metodai. Apžvelgti kitų mokslininkų atlikti tyrimai, aprašyti gauti rezultatai. Pateikiama informacija apie bevielio

interneto prieigos Wi-Fi galimas grėsmes. Detaliai aprašomi Wi-Fi saugos protokolai: WEP, WPA, WPA2. Šios dalies pabaigoje pateiktos apibendrintos išvados.

Projektavimo dalyje pateiktas tyrimo srities apibrėžimas, tyrimo modelis bei metodika. Aprašyta programa: sudaryta panaudos atvejų diagrama, blokinės schemos, aprašytos naudojamos klasės.

Eksperimentinėje dalyje aprašytas energijos suvartojimo, panaudojant Wi-Fi saugos protokolus, tyrimas, jo atlikimo eiga ir pateikiami skaitiniai bei grafiniai tyrimo rezultatai. Aprašomos eksperimento išvados.

Pabaigoje pateikiamos bendros darbo išvados ir rezultatai.

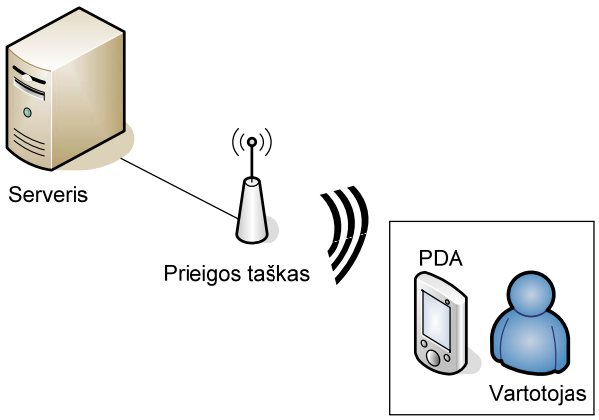
Prieduose pridėta kita su darbu susijusi informacija.

Magistrinio darbo tematika parašytas straipsnis išspausdintas leidinyje „Informacinės technologijos. XVI tarpuniversitetinė magistrantų ir doktorantų konferencija.“ Bei pristatytas pranešimas XVI tarpuniversitetinėje magistrantų ir doktorantų konferencijoje, vykusioje 2011-04-22 Kaune.

1 MOBILIŲJŲ INFORMACINIŲ SISTEMŲ APSAUGOS IR ENERGIJOS SĄNAUDŲ SPRENDIMŲ ANALIZĖ

1.1 Bevielių tinklų problema ir paplitimas

Išaugęs nešiojamų kompiuterių su Wi-Fi technologija, delninių ir mobiliųjų telefonų su galimybe jungtis prie interneto paplitimas[1], įtakojo Wi-Fi viešosios prieigos taškų tinklo plėtimąsi. Jie įrengti daugelyje viešųjų vietų, tokių kaip mokymosi įstaigos, bibliotekos, oro uostai, prekybos centrai. Tačiau viešasis internetas nėra saugus, nes jame nenaudojamos saugumo priemonės. 1 paveiksle parodyta Wi-Fi prieiga, kai naudotojas turintis delninuką naudojasi prieigos tašku, kad prisijungtų prie interneto paslaugų. Srautas, keliaujantis nuo naudotojo iki prieigos taško yra atviras, nešifruotas. Kadangi ši technologija pagrįsta radijo bangų veikimu, piktavaliai gali lengvai įsiterpti tarp šios dalies ir įvykdyti „žmogaus viduryje“ (angl. Man in the middle) ataką. Todėl atliekant operacijas su svarbiais duomenimis viešajame internete, siūloma imtis saugumo priemonių. Šios priemonės įtakoja energijos suvartojimą, todėl baterijas reikia dažnai įkrauti.

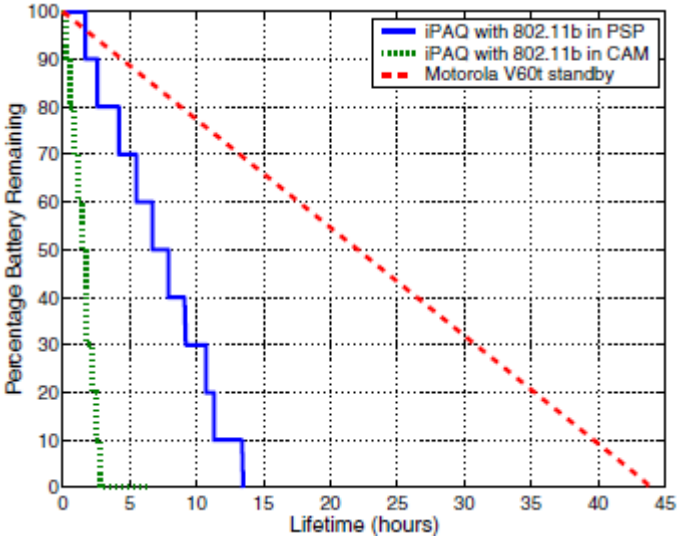


1 paveikslas. Delninuko jungimasis per Wi-Fi prie kompiuterių tinklo

Bevielė technologija suvartoja apie 10% visos energijos dabartiniuose nešiojamuose kompiuteriuose. Delninukuose jos suvartojimas siekia apie 50% [1,2,3].

Nors PDA turi daug privalumų lyginant su mobiliaisiais telefonais, šie lenkia PDA bent vienoje srityje – elektros energijos suvartojimo. Delniniai kompiuteriai gerai nevaldo energijos naudojimo ir tai greitai išsekina jų baterijas [5]. Didelė dalis energijos sunaudojimo priskiriama bevielei LAN tinklo kortelei. Naudojant WiFi technologiją, PDA prijungiamas prie IEEE 802.11b bevielio LAN tinklo, per kelias valandas išeikvoja bateriją. Priešingai, mobiliųjų telefonų baterijos veikimo laikotarpis yra net kelios dienos. Tai pavaizduota 2 paveiksle, kuriame delninio kompiuterio, naudojančio bevielę technologiją, budėjimo laikas (Compaq iPAQ H3650 su IEEE 802.11b korta) palyginamas su GSM mobiliojo telefono

(Motorola V60t) budėjimo laiku. Delninis kompiuteris pavaizduotas dvejais atvejais. Pirmu, bevielio ryšio kortelė visada yra aktyvi, antru atveju, bevielio ryšio kortelė yra energijos taupymo rėžime (aprašytas 1.3.1 skyriuje). Pastebime, kad delninio kompiuterio su bevieliu LAN baterijos tarnavimo laikas tris kartus mažesnis nei mobilaus telefono.



2 paveikslas. *Budėjimo trukmė iPAQ su IEEE 802.11b korta aktyviame rėžime ir taupymo rėžime palyginant su mobiliojo telefono tarnavimo laiku.*

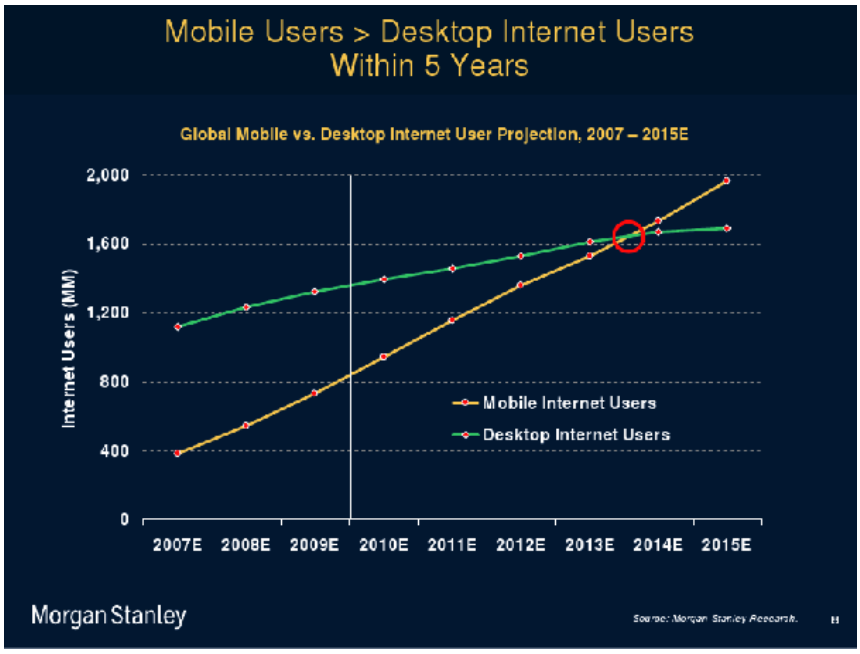
2010 metais portalo „AnandTech.com“atliktame tyrime [26], buvo palyginti tuo metu populiariausių parduodamų išmaniųjų telefonų baterijų veikimo laikai naršant internetą prisijungus prie bevielio interneto taško. Gauti rezultatai parodė, kad skirtingų modelių baterijų veikimo laikas buvo nuo 5 iki 10 valandų.

1.2 Mobiliojo darbo augimas

Mobiliojo interneto rinka auga milžiniškais tempais. Didelę įtaką šiam augimui daro išmaniųjų telefonų, kuriais naudojamasi internetu, pardavimų augimas. Spėjama, kad iki 2014 metų apie 90 procentų visų išmaniųjų telefonų turės įdiegtą Wi-Fi technologiją [25].

Rinkų analitikai [24] mano, kad šių metų pabaigoje naudojamų išmaniųjų telefonų skaičius pralenks kompiuterių skaičių. Pagal „International Data Corp“ (IDC) duomenis paskutinį 2010 m. ketvirtį išmaniųjų telefonų rinkai buvo pateikta 101 mln. (87% augimas, lyginant su atitinkamu prieš tai buvusių metų laikotarpiu), o asmeninių kompiuterių - 92 mln. (augimas - mažiau 3%). Po dviejų metų mobiliuoju internetu besinaudojančių vartotojų skaičius turėtų pralenkti fiksuotojo interneto vartotojus [23]. 3 paveikslo grafike pavaizduotas interneto paslaugų didėjimas tiek mobilaus interneto naudotojų tarpe, tiek asmeninių kompiuterių interneto naudotojų. Matosi, kad vis labiau populiarus tampa mobilus internetas, jo naudojimo tempas sparčiai kilo nuo 2007 metų ir tebekyla. Asmeninių kompiuterių interneto naudojimas nuo 2007 metų augo ne tokiais dideliais tempais ir numatomas jo

tolimesnis lėtas augimas. Tai parodo, kad šiuolaikiniai naudotojai vis labiau prisiriša prie mobiliųjų įrenginių, kurių pagalba galima atlikti daugybę funkcijų ir operacijų, kad ir kur naudotojas bebūtų (angl. Work on the go): internetinės paslaugos, žiniatinklių peržiūra, dokumentų tvarkymas, grafinės pramogos ir kt.



3 paveikslas. Mobilaus interneto ir asmeninių kompiuterių interneto naudojimo grafikas

1.3 Egzistuojantys bevielių tinklų energijos taupymo sprendimai

1.3.1 IEEE 802.11b energijos taupymo rėžimas mobiliems įrenginiams

802.11b specifikacija kontroliuoja duomenų persiuntimus tarp fizinio sluoksnio (radijo ryšio) ir jo apibrėžto prieigos prie terpės valdymo (MAC) sluoksnio. Tinklas palaiko visas MAC sluoksnio funkcijas keisdamasis kontrolės kadrų serijomis, prieš tai leisdamas siųsti duomenis aukštesniems sluoksniams. Jis taip pat nustato kelis parametrus tinklo adapteriui. Vienas iš jų yra energijos rėžimas.

Tinklo adapteris palaiko du rėžimus: aktyvų rėžimą (angl. Active mode) ir energijos taupymo rėžimą (angl. Power save polling mode). Pirmajame rėžime radijo imtuvas yra aktyvioje būsenoje ir visada vartoja energiją, tai leidžia jam priimti duomenis bet kuriuo laiku. Antrajame imtuvas dažniausiai būna laukimo būsenoje, tačiau periodiškai duoda užklausą prieigos taškui dėl naujų pranešimų. Todėl šis rėžimas sumažina baterijos energijos suvartojimą nešiojamuose ir delniniuose kompiuteriuose[1,2,4].

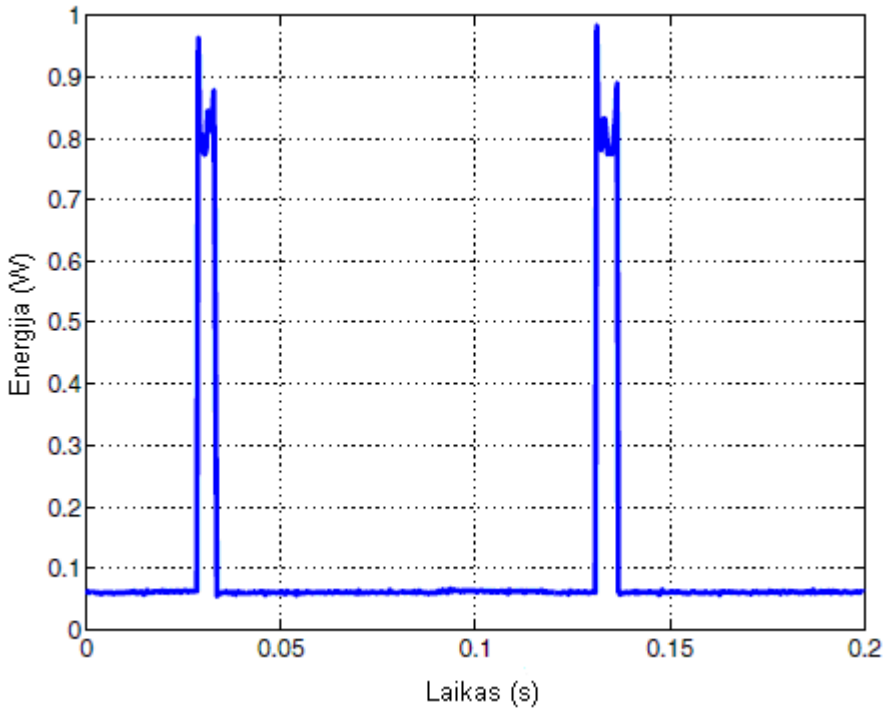
E.Shin, P.Bahl ir M.J.Sinclair darbe nagrinėjo energijos suvartojimą, tyrimui atlikti pasirinkus ORiNOCO PC Gold ir Cisco AIR-PCM350 bevielio tinklo kortas[5]. Galimos aktyvi, budėjimo ir išjungta (off) būsenos. Aktyvioje būsenoje korta gali būti trijų būsenų: perdavimo, priėmimo ir laukimo. Budėjimo ar miego būsenoje, korta yra nenaudojama ir

negali siųsti ar priimti duomenų. Remiantis matavimų analizės metodiką, 1 lentelėje pateiktas nustatytas energijos suvartojimas esant skirtingom kortos būsenom. Iš lentelės matome, kad miego būsenoje energijos suvartojimas yra žymiai mažesnis nei kitose būsenose. IEEE 802.11b energijos taupymo rėžimas stengiasi pasinaudoti šiuo skirtumu, kad sumažintų energijos sąnaudas.

1 lentelė. Bevielio tinklo būsenų energijos suvartojimas

Būsena Korta	Miego (mA)	Laukimo (mA)	Gavimo (mA)	Perdavimo (mA)
ORiNOCO PC Gold	12	161	190	280
Cisco AIR-PCM350	9	216	260	375

Pateiktame 3 paveikslo grafike matosi energijos kiekis per vieną energijos taupymo rėžimo ciklą, atliktą su ORiNOCO PC Gold korta. Tikrinimo intervalas (Listen interval) kas 100ms.



4 paveikslas. *ORINOKO PC Gold kortos energijos suvartojimas, pasinaudojus energijos taupymo rėžimu, kai miego būsenos trukmė 100ms.*

1.3.2 IEEE 802.11v bevielio tinklo standartas su energijos taupymo savybe

Dabartinės bevielės technologijos, turinčios didelį duomenų pralaidumą, sudaro sąlygas dideliems energijos kiekiams plisti oru, atliekant nuolatinį duomenų perdavimą. Atsižvelgdamas į šias sąlygas IEEE komitetas parengė naują Wi-Fi standartą, kuriame daugiausiai dėmesio skiriama elektros energijos vartojimo mažinimui bevielio tinklo prietaisuose[2].

Viena iš patraukliausių funkcijų – bevielio tinklo miego būsenos valdymas, kuris leidžia ilgesnę miego būsenos trukmę bevieliams įrenginiams. Tai sutaupo didesnę dalį energijos, palyginus su įprastais maršrutizatoriais ar bevieliais prietaisais. Be sugebėjimo nustatyti bevielio ryšio prietaisą į laukimo (idle) būseną, protokolas taip pat gali jį pažadinti be naudotojo įsikišimo.

1.4 Bevielio ryšio įrenginio energijos sąnaudas mažinantys metodai

1.4.1 Dinaminis energijos valdymo metodas

Dinaminis energijos valdymo (angl. Dynamic power management - DPM) metodas skirtas sutelkti dėmesį į bevielio tinklo kortos kontrolę, sumažinant energijos suvartojimą jos veikimo metu[6,7].

DPM apima metodų rinkinį, kurie siekia efektyvaus energijos vartojimo mažėjimo, išjungiant visus ar tik mažinant vykdomų sistemos komponentų skaičių, kai jie yra laukimo būsenoje. Energijos valdymo sistemoje komponentus galima nustatyti į skirtingas būsenas, kuriose kiekviena pasižymėtų skirtingomis savybėmis ir energijos naudojimo lygiu. Pavyzdžiui, sistemos komponentai gali turėti aktyvią būseną, laukimo būseną ir miego būseną, kuriose energijos vartojimas yra minimalus. Perėjimas tarp šių būsenų yra kontroliuojamas energijos valdymo modulio, kuris stebi sistemos apkrovą ir atsižvelgiant į anksčiau atliktus sistemos veiksmus, darbo krūvį ir veiklos apribojimus, nusprendžia, kuriuo laiku, kokia būsena bus pasirinkta.

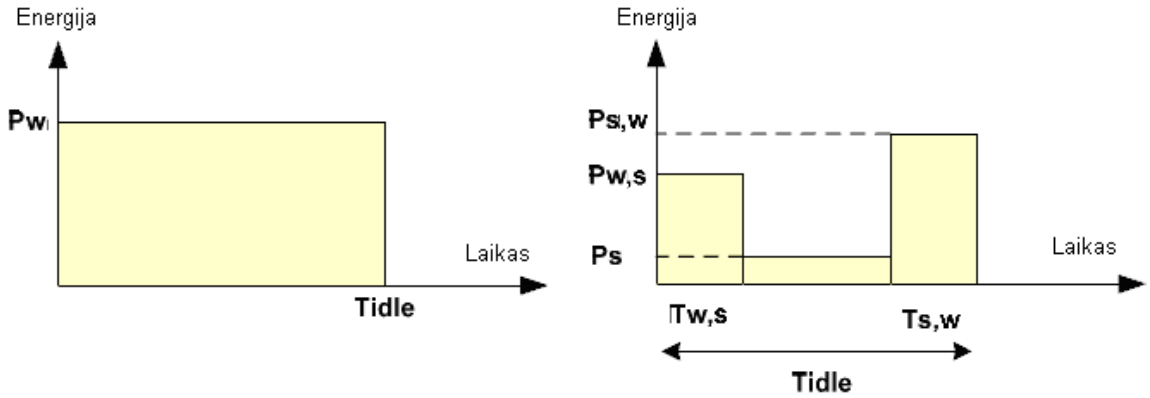
Dažniausiai naudojamas DPM algoritmų rinkinys paremtas pertrūkių strategija. Jų trūkumas tas, kad jie nereikalingai naudoja energiją, laukdami, kol pereis į mažai energijos naudojančią būseną. Antras DPM algoritmų rinkinys remiasi elgesio prognozavimu sekančiam laiko periodui. Komponentas bus dedamas į mažos energijos rėžimą, jeigu jis nėra šiuo metu naudojamas ir valdymo modulis prognozuoja didesnį neveiklumo laiką. Trečias algoritmų rinkinys yra atsitiktinių algoritmų, kurie remiasi komponento prašymo aktyvuoti pasiskirstymu. Šie pasiskirstymai gaunami modeliuojant ar stebint įvykius sistemoje per tam tikrą laikotarpį[7].

4 paveikslas parodo suvartojamą energiją be DPM technologijos ir su ja. Prastovos laikas (idleTime) yra minimalus laiko tarpas sistemai pereiti į laukimo būseną, kuri garantuotų energijos taupymą. Galima apskaičiuoti mažiausią priimtiną prastovos laiko vertę ir palyginti sunaudojamą energiją abejais atvejais. Rezultatas apskaičiuojamas lygtimi:

$$T_{idle} = \frac{P_{w,s}T_{w,s} + P_{s,w}T_{s,w} - P_s(T_{w,s} + T_{s,w})}{P_w - P_s}$$

Kur,

- Pw: energijos sunaudojimo vidurkis darbo būsenoje;
- Ps: energijos sunaudojimo vidurkis miego būsenoje;
- Tw,s: perėjimui iš darbo į miego būsena sugaištas laikas;
- Ts,w: perėjimui iš miego į darbo būseną sugaištas laikas;
- Pw,s: energijos sunaudojimas pereinant iš darbo į miego būseną.
- Pw,s: energijos sunaudojimas pereinant iš miego į darbo būseną.



5 paveikslas. Energijos suvartojimo palyginimas veikimo būsenoje ir laukimo būsenoje

Jeigu laukimo periodas bus ilgesnis už prastovos laiką (idleTime), energijos sutaupymas bus akivaizdus. Tačiau, iškyla problema, kaip numatyti laukimo periodo trukmę prieš jam prasidedant.

1.4.2 Tiesiniu prognozavimu pagrįstas metodas

Bevieliame tinkle tarp serverio ir kliento perduodami duomenų paketai kaip atskiros eilutės. Tarp dviejų gretimų eilučių yra tarpas, per kurį neperduodami jokie duomenys. Kiekvieno tarpo ilgis nustatomas pasitelkus daugelį su tinklo srautu susijusių veiksnių. Šie tarpai taip pat yra laiko tarpai. Taigi, Y.Wei, S.Chandra ir S.Bhandarkar sukūrė statistinį tiesiniu prognozavimu pagrįstą metodą (Linear prediction based approach), kuriuo galima nuspėti būsimų tarpų ilgio reikšmę atsižvelgiant į ankstesnes pastabas[3]. Tiesinis duomenų prognozavimas yra matematinė operacija, kurioje būsima laiko tarpo vertė apskaičiuojama kaip tiesinė funkcija nuo anksčiau buvusio pavyzdžio. Šią funkciją galima užrašyti:

$$x'(n) = \sum_{i=1}^{p} a_i x(n-i),$$

kur, x'(n) – apskaičiuotas tarpo ilgis, x(n-i) – anksčiau buvusi reikšmė, a_i – numatomas koeficientas. Klaida generuojama pagal formulę:

$$e(n)= x(n) – x'(n),$$

kur, x(n) yra tikroji reikšmė, o x'(n) apskaičiuota tarpo ilgio reikšmė.

Tiesinis prognozavimas optimizuoja įvertinimą, mažindamas jų klaidas. Jis turi du reguliuojamus parametrus: polių skaičių p ir laiko intervalo plotį, naudojamą apskaičiuojant numatomo koeficiento reikšmę. Šiems parametrams reikia atlikti bandymus norint pasirinkti tinkamiausią reikšmę.

Jei prognozuojamas tarpo ilgis bus ilgesnis nei faktinis, bevieliame tinkle naudotojas pastebės duomenų srauto parsisiuntimo vėlavimą, nes daugelis paketų keliaus pas naudotoją kol WLAN bus miego būsenoje. Todėl naudinga įtraukti mažas paklaidas prie miego trukmės ilgių (numatomų tiesinio prognozavimo metodo), siekiant sumažinti duomenų praleidimo greitį. Tačiau, jei paklaida bus per didelė (pagal dydį) sutaupyti baterijos energijos nepavyks.

Tiesinio prognozavimo metodas pateikia tikslesnes paklaidas miego intervalo ilgiams, palyginus su paprastu, istorija pagrįstu, prognozės metodu, kuris numato dabartinį miego intervalo ilgį kaip paprastą vidurkį iš prieš tai buvusių miego intervalų ilgių reikšmių. Vadinasi, paklaida, naudojama tiesinio prognozavimo metode, dažniausiai yra mažesnė (pagal dydį) nei paprasto prognozės metodo. Tai reiškia, kad šis metodas sutaupo daugiau energijos.

Y.Wei, S.Chandra ir S.Bhandarkar atliko eksperimentą tarp multimedijos serverio su bevieliu prieigos tašku ir kliento, naudojančio mobilų įrenginį su bevielio tinklo plokšte. Eksperimentas detaliai aprašomas literatūroje pateiktame straipsnyje[3]. Gauti rezultatai parodė, kad šiam metodui suteikta paklaidos vertė sumažino duomenų greitį, tačiau sumažėjo ir energijos suvartojimo rodiklis, palyginus su paprastos prognozės metodu.

1.5 Wi-Fi saugos mechanizmų veikimas

Norint, kad Wi-Fi bevielis ryšys užtikrintų saugų informacijos persiuntimą, naudojami bevielio tinklo saugos mechanizmai[14,15]. Kiekvienas bevielio perdavimo saugumo mechanizmas sukurtas užtikrinti tris pagrindines funkcijas [13]: autentiškumo, patikrinti tapatumą stoties, su kuria yra bendraujama; konfidencialumo (privatumo) užtikrinimui, kad belaidžiu tinklu perduodama informacija išliktų privati ir apsaugota; vientisumui užtikrinti, kad perduodami MAC kadrai (angl. MAC Protocol Data Unit) nepažeisti pasiektų tikslą. Autentifikacija veikia tarp Wi-Fi stočių.

1.5.1 WEP saugos protokolas

Pirmasis buvo sukurtas WEP protokolas, kuris stengėsi suderinti konfidencialumo, prieigos kontrolės ir duomenų vientisumą bevieliame tinkle[8]. Deja, protokole buvo rasta trūkumų. WEP (angl. Wired Equivalent privacy) konfidencialumui (privatumui) užtikrinti naudoja RC4 šifravimo algoritmą. RC4 yra srautinis šifras, kuris veikia plėsdamas trumpą raktą į begalinį pseudo atsitiktinį srautinį raktą. Siekiant išvengti dviejų tekstų su tuo pačių

srautiniu raktu, naudojamas inicializacijos vektorius (IV), kuris sustiprina bendrą slaptą raktą ir kiekvienam paketui sukuria skirtingus raktus. Inicializacijos vektorių sudaro 24 bitai, jis suteikia 64 ar 124 bitų raktą.

MAC kardų vientisumo užtikrinimui WEP naudoja vientisumo kontrolinių sumų (angl. Integrity Check Value – ICV) mechanizmą. Jis įgyvendina 32 bitų ciklinę pertekliaus kontrolę (CRC-32). Kiekvienam siunčiamam MAC kadrui apskaičiuojama CRC kontrolinės suma, kuri pridedama jo pabaigoje. Jei CRC, kuri buvo apskaičiuota šaltinio ir išsiųsta su žinute, yra tokia pati kaip gavėjo iš naujo apskaičiuota, toks pranešimas galios ir bus perduotas perdavimo kanalo lygiui, o jei suma gauta skiriasi, gaunamas vientisumo pažeidimas ir žinutė yra pašalinama.

WEP turi dviejų rūšių autentifikavimą: atvirą (angl. Open system) arba bendro rakto (angl. Shared-Key). Tiesa, atviras nėra autentiškumo procedūra, nes tada prieigos taškas (angl.Access point) priima kiekvieną stotelę be tapatybės patikrinimo. Taigi, stotis pasikeičia su AP dvejomis žinutėmis, kurių viena nurodo tapatybę, kita prašymą patvirtinti. Prieigos taškas atsako, patvirtindamas sėkmingą autentifikaciją. Po atpažinimo ir susiejimo, WEP gali būti naudojamas duomenų šifravimui, tada klientui reikia turėti atitinkama raktą. Bendro rakto autentifikacijai prisijungimui reikia slapto rakto. Šiuo atveju, autentiškumui pasiekti, stotis pradeda keturių krypčių pranešimų keitimąsi.

WEP saugos protokolo duomenys apibendrinti pateikti 2 lentelėje.

2 lentelė. Bevielio tinklo WEP saugos protokolo parametrai

WEP		
Autentifikacija	Metodas	Atvira sistemos autentifikacija Bendro rakto autentifikacija
Rakto šaltinis ir valdymas	Raktas	Šifravimo raktas: 40 bitų bendras raktas ir 24 bitų IV, viso – 64 bitų raktas. 104 bitų bendras raktas ir 24 bitų IV, viso – 128 bitų raktas.
Konfidencialumas	Duomenų srauto šifravimas Šifro algoritmai srauto duomenims ir raktų dydžiui Užšifruoti kadrai	– RC4 su 64 bitų raktu (WEP-40) RC4 su 128 bitų raktu (WEP-104) MPDU + ICV
Vientisumas	Vientisumo algoritmas Apsaugoti kadrai	32 bitų ICV su CRC-32 MPDU

1.5.2 WPA saugos protokolas

Buvo įrodyta, kad WEP neužtikrina saugumo. Jo trūkumai: RC4 turi silpną rakto rėžimą, kriptografinis raktas ir inicializacijos vektorius yra trumpi ir negali būti automatiškai

ir dažnai atnaujinami, CRC-32 neužtikrina vientisumo ir yra neatsparus atakoms. Dėl šių priežasčių buvo sukurtas WPA (angl. WiFi Protected Access), kuris yra dalis 802.11i standarto.

Konfidencialumui ir vientisumui užtikrinti WPA naudoja laikinojo rakto vientisumo protokolą (TKIP), kuris saugiai keičia WEP raktą su lig kiekvienu duomenų paketu. Tokiu būdu kodavimas užveria kelią slaptam pasiklausymui[13]. Tačiau kaip ir WEP protokolas, užšifravimui ir iššifravimui naudoja RC4 šifrą, tik siekiant užtikrinti didesnį saugumą TKIP padidina inicalizacijos vektoriaus lauką iki 48 bitų. TKIP naudoja sumaišytą raktą, sudarytą iš laikino rakto, siuntimo adreso ir sekos skaitiklio TSC. Taip užtikrinama, kad kiekvienas duomenų paketas siunčiamas su savo unikaliu šifravimo raktu.

Autentifikavimui naudojamas 802.1X autentifikavimo protokolo mechanizmas arba iš anksto padalintų raktų metodas (angl. Pre-Shared Key – PSK), kuris skirtas bevielio ryšio sesijų metu identifikavimo raktams kurti. PSK numatytas naudoti mažuose namų arba ofisų tinkluose, kuriuose kritiškas autentifikavimas nėra svarbus. PSK metodui būtini du komponentai – klientas bei autentifikatorius. Prieigos taškas naudodamas PSK yra atsakingas tik už kliento priėmimą į tinklą[13].

Duomenų vientisumui tikrinti CRC algoritmą pakeitė MIC (abgl. Micheal) algoritmas (64 bitų žinutė). CRC algoritmas, naudotas 802.11 protokole yra nesunkiai apeinamas. MIC algoritmas šiuo atveju yra žymiai stipresnis. Duomenų teisėtumo procedūros tikrina duomenis nuo žalingų bei atsitiktinių duomenų perdavimo iškraipymų. 802.1X kur kas saugesnis nei PSK, tačiau tam reikia turėti RADIUS autentifikavimo serverį (3 lentelė).

3 lentelė. Bevielio tinklo WPA saugos protokolo parametrai

WPA		
Autentifikacija	Metodas	802.1X autentifikacija Bendro rakto autentifikacija
Rakto šaltinis ir valdymas	Raktas	TKIP. 48 bitų IV laukas naudojamas kaip MPDU TKIP sekos skaitiklis (TSC).
Konfidencialumas	Duomenų srauto šifravimas Šifro algoritmai srauto duomenims ir raktų dydžiui Užšifruoti kadrai	– RC4 su 256 bitų raktu. MPDU + MIC + ICV
Vientisumas	Vientisumo algoritmas Apsaugoti kadrai	1) 64 bitai Michael (MIC). 2) 32 bitai ICV [MIC]: (MSDU angl. MAC service data unit) siuntėjo ir gavėjo adresai, MSDU pirmenybė, ir MSDU naudingoji apkrova. [ICV]: MPDU

1.5.3 WPA2 saugos protokolas

WPA buvo tik laikinas sprendimas, todėl pagrindinės WEP problemos paskatino IEEE 802.11i standarto sukūrimą ir jo realizavimą kaip WPA2 protokolą.

Konfidencialumui bei vientisumui užtikrinti WPA2 naudoja skaitiklio rėžimą su CBC-MAC protokolu (angl. Counter-Mode/Cipher Block Chaining – CCMP). Šifravimui ir duomenų vientisumui CCMP naudoja AES šifrą su 128 bitų raktu ir 128 bitų bloko dydžiu.

Vientisumui užtikrinti, CCM-MAC operacijos išplečia pradinį MPDU dydį iki 16-8 baitų CCMP antraštei ir 8 baitų MIC laukui. CCM reikalauja naujo laikino rakto kiekvienai sesijai ir unikalios reikšmės kiekvienam kadrui. Šiam tikslui naudojamas 48 bitų paketas. CCM nenaudoja WEP kontrolinių sumų mechanizmo (ICV). CCM apsaugo papildomus autentiškumo duomenis, kurie sudaryti iš MPDU antraštės ir apima polaukius iš MAC kadro kontrolės, šaltinio adresus ir paskirties laukus, sekos kontrolę, QoS kontrolės lauką, todėl užtikrinama didesnė vientisumo apsauga.

Autentifikavimui naudojamas 802.1X autentifikavimo protokolo mechanizmas arba iš anksto padalintų raktų metodas PSK.

4 lentelė. Bevielio tinklo WPA2 saugos protokolo parametrai

WPA2		
Autentifikacija	Metodas	802.11X autentifikacija su (RADIUS) serveriu. Bendro rakto autentifikacija
Rakto šaltinis ir valdymas	Raktas	PMK generuoja individualų laikiną raktą PTK, iš kurio gaunami trys raktai: 1-2) 128 bitų, 3) 256 arba 128 bitų.
Konfidencialumas	Duomenų srauto šifravimas Šifro algoritmai srauto duomenims ir raktų dydžiui Užšifruoti kadrai	Laikino rakto šifravimas: 1) RC4 su 128 bitų šifravimo raktu, 2) su AES 128 bitų šifravimo raktu. AES-CCM su 128 bitų laikinu raktu. MPDU +MIC
Vientisumas	Vientisumo algoritmas Apsaugoti kadrai	1) 64 bitai CCM MIC pranešimų srautui 2 a) HMAC-MD su pagrindiniu patvirtinimo raktu, b) HMAC-SHA1 su 128bitų pagrindiniu patvirtinimo raktu pasisveikinimui. [MIC]:MPDU+papildomas duomenų autentiškumo tikrinimas, kurį sudaro MPDU antraštė, polaukiai iš MAC kadrų kontrolės, šaltinio ir paskirties adresai, sekos kontrolė, QoS kontrolės laukas. [HMAC]: 4kartų pasisveikinimas.

Jei naudojamas bendras raktas PSK, sukurti individualų pagrindinį raktą PMK, naudojamas slaptažodis. PMK generuoja individualų laikiną raktą PTK, iš kurio gaunami trys raktai. 1) 128 bitų raktas autentifikavimo procedūrai. 2) 128 bitų raktas šifravimui, kuris reikalingas srautinio rakto konfidencialumui per „rankų paspaudimą“ su AES. 3) 256 bitai TKIP arba 128 bitai laikinam raktui AES-CCMP. Jis naudojamas WPA2 konfidencialumui.

Šie bevielio tinklo saugos protokolo duomenys apibendrinti 4 lentelėje.

1.6 Wi-Fi grėsmių analizė

Pasyvių atakų [13], tokių kaip slaptas pasiklausymas ar srauto analizė, nėra išvengiama naudojant saugos protokolus. Tačiau aktyvių atakų [13] atžvilgiu, žymiai saugesnis yra WPA2 protokolas. Šios atakos apibendrintos pateiktos 5 lentelėje.

TKIP protokolas jau yra laikomas pažeidžiamu [16,17], todėl neapsaugo nuo slapto pasiklausymo ar pakartotinų atakų. Dėl šio pažeidžiamumo WPA protokolas tapo ne toks saugus kaip WPA2. Tačiau jei yra galimybė tinklą sukonfigūruoti pasirinkus AES-CCMP parametrus, WPA bus veiksmingas [16].

5 lentelė. WiFi grėsmių analizė

IEEE protokolas		WiFi		
		WEP	WPA	WPA2
Pasyvios atakos	Slaptas pasiklausymas	Negali būti išvengta. 1)Srauto modeliai gali nustatyti ryšio turinį (vaizdo konferencijas, pranešimų žinutes). 2) Stotelių ir prieigos taškų MAC adreso perėmimas.	Negali būti išvengta. 1)Srauto modeliai gali nustatyti ryšio turinį (vaizdo konferencijas, pranešimų žinutes). 2) Stotelių ir prieigos taškų MAC adreso perėmimas.	Negali būti išvengta. 1)Srauto modeliai gali nustatyti ryšio turinį (vaizdo konferencijas, pranešimų žinutes). 2) Stotelių ir prieigos taškų MAC adreso perėmimas.
	Srauto analizė	Negali būti išvengta.	Negali būti išvengta.	Negali būti išvengta.
Aktyvios atakos	Rakto nulaužimas	Galimas RC4 rakto nulaužimas.	Galimas RC4 rakto nulaužimas	AES suteikia saugumą – negalimas rakto nulaužimas
	Vartotojo autentifikavimo pažeidimas	1) Bendro rakto autentifikacija silpna dėl RC4 (brutalios, žodyno atakos) 2) Mikroprogramos pakeitimas lemia autentifikavimo pažeidimą.	1) Bendro rėkto autentifikacija silpna dėl RC4. 2) Mikroprogramos pakeitimas lemia autentifikavimo pažeidimą. 3) 802.1X labai saugus.	1) Mikroprogramos pakeitimas lemia autentifikavimo pažeidimą. 2) 802.1X labai saugus.
	Apsimetimas (angl. Masquerading, spoofing)	1)Stoties apsimetimas 2) Prieigos taško apsimetimas	1)Stoties apsimetimas 2) Prieigos taško apsimetimas (kai nenaudojamas 802.1X).	802.1X autentifikacija labai stipri, bet sesijos užgrobimas (angl.hijacking) galimas po 3 žinutės iš prieigos taško sėkmingam EAP.
	Pakartotinos atakos	Galimos, nes nėra jokio mechanizmo, kad būtų užkirstas kelias pakartotinoms atakoms.	48 bitų TKIP sekos skaitiklis (TSC), užkirsti kelią pakartotinoms atakoms.	48 bitų paketo skaitiklis, užkirsti kelią pakartotinoms atakoms.
	Žinutės modifikavimo atakos	CRC-32 silpnas apsaugoti nuo tokių atakų	1) CRC-32 silpnas apsaugoti nuo tokių atakų 2) MIC apsaugo nuo tokių atakų MSDU.	CCMP numato saugumą nuo modifikuotų atakų.
	DoS atakos (fizinis sluoksnis)	Tyčinis trikdymas	Tyčinis trikdymas	Tyčinis trikdymas
	DoS atakos (MAC sluoksnis)	1) Tinklo blokas su CSMA/CA išnaudojimu 2) Autentifikacijos nuėmimo ataka 3) Tyčinės CRC klaidos	1) Tinklo blokas su CSMA/CA išnaudojimu 2) Autentifikacijos nuėmimo ataka 3) Tyčinės CRC klaidos	1) Tinklo blokas su CSMA/CA išnaudojimu 2) Autentifikacijos nuėmimo ataka

1.7 „Bluetooth“ ir „Wi-Fi“ technologijų suvartojamos energijos palyginimas

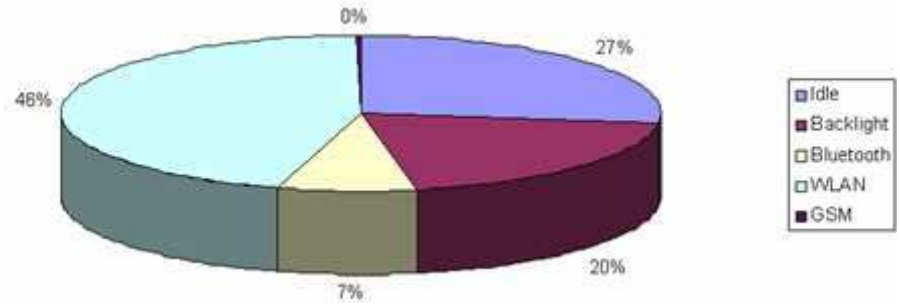
Dažnai sutinkamos mažo nuotolio bevielės technologijos yra Bluetooth ir IEEE 802.11b (Wi-Fi). Bluetooth technologiją palaikantys prietaisai gali būti nutolę iki 10metrų nuo siunčiamo signalo, o duomenys tarp įrenginių, priklausomai nuo jų tipo, gali būti perduodami 1-3Mbps sparta. Vienas pagrindinių privalumų yra mažas energijos suvartojimas: duomenų perdavimui ir priėmimui nuo 100 iki 200 mW, laukimo būsenai nuo 10 iki 20 mW.

IEEE 802.11b turi ilgesnį veikimo nuotolį – apie 100metrų, jo sparta siekia 11Mbps, todėl sunaudojama daugiau energijos. Bevielio kompiuterio tinklo plokštė sunaudoja apie 60mW miego būsenoje, 805 mW laukimo būsenoje, 950 mW priiminėdamas duomenis ir 1400 mW perduodamas duomenis[10].

Taigi energijos sąnaudų sumažinimas, veikiant belaidžiai technologijai, pasiekiamas praleidžiant kiek įmanoma daugiau laiko žemos energijos rėžime.

1.8 Fujitsu-Siemens Loox T830 delninuko komponentų energijos suvartojimo tyrimas

D.Tudor ir M.Marcu atliko tyrimą apie skirtingų komponentų energijos suvartojimą [7]. Tyrimas buvo atliktas su delniniu kompiuteriu Fujitsu-Siemens Loox T830. Gauti rezultatai pavaizduoti diagramoje 6 paveiksle, iš kurio matosi, kad bevielis ryšys (WLAN) sunaudoja daugiausiai energijos – 46%. Procesorius ir atmintis (idle) suvartoja 27% energijos, ekranas (backlight) – 20%, „Bluetooth“ technologija – 7%, „GSM“ technologija– 20%.



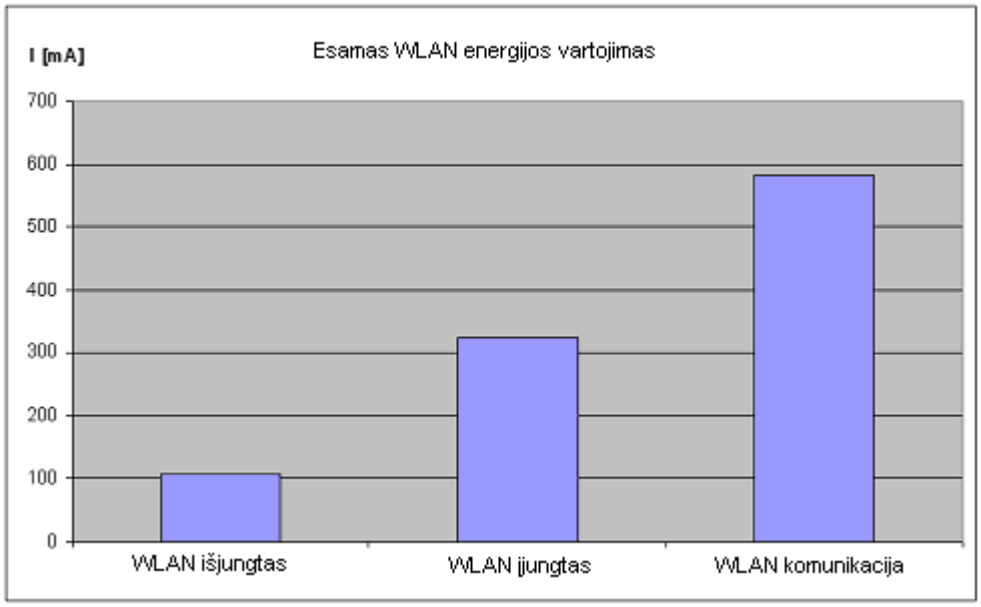
6 paveikslas. Mobiliojo telefono energijos sąnaudų pasiskirstymas

Tyrime paaiškėjo, kad didžiąją dalį elektros energijos suvartoja WLAN. Siekiant parodyti WLAN energijos suvartojimą kitu aspektu, kita tyrimo dalis buvo atlikta su Loox N560 delninuku:

- WLAN išjungtas;
- WLAN įjungtas, bet neprijungtas prie tinklo;
- WLAN įjungtas ir bando prisijungti prie tinklo;
- WLAN įjungtas ir prisijungia prie tinklo;

- WLAN įjungtas ir siunčia duomenis tinklu.

7 paveiksle pavaizduotas energijos naudojimas kai WLAN yra išjungtas, kai įjungtas ir kai vyksta WLAN komunikacija. Įjungtas WLAN turi tokias pačias energijos sąnaudas nepriklausomai nuo WLAN tinklo būsenos: neprijungtas, bando prisijungti prie tinklo ir prisijungus.



7 paveikslas. WLAN vartojimo klasės

Taigi daugiausiai energijos suvartojama, kai bevielis tinklas yra įjungtas ir siunčia duomenis tinklu.

1.9 Analizės išvados

- Wi – Fi technologijos paplitimas, įtakojo mobilaus darbo augimą, nes naudotojai nori būti nuolat prisijungę prie interneto ryšio ir naudotis savo duomenimis visur ir visada.
- Išmaniuosiuose telefonuose bevielė technologija suvartoja apie 50% baterijos energijos.
- Maksimalus baterijos laikas, naršant internetą prisijungus prie bevielio ryšio interneto taško priklauso nuo delninuko modelio ir svyruoja tarp 5-10 valandų.
- Informacijos saugą, informaciją perduodant bevieliu ryšiu, užtikrina saugos protokolai: WEP, WPA, WPA2. Jie išanalizuoti ir pateikti šioje dalyje.
- Aprašytas IEEE 802.11b energijos taupymo rėžimas, kuris sumažina baterijos energijos suvartojimą nešiojamuose ir delniniuose kompiuteriuose.
- Pateiktas dinaminis energijos valdymo metodas, kuris sumažina bevielio tinklo kortos energijos suvartojimą jos veikimo metu.

- Aprašytas tiesiniu prognozavimu pagrįstas metodas, kuris sumažina energijos suvartojimą.
- D.Tudor ir M.Marcu atliktame tyrime nustatyta, kad bevielė technologija suvartoja daugiausiai energijos – 46%.
- Tikslių duomenų apie sunaudotos energijos kiekį, kai įjungtas vienas ar kitas saugos protokolas, naudojant Wi-Fi, nėra, todėl tikslinga atlikti tyrimą.

2 DELNINIŲ KOMPIUTERIŲ ENERGIJOS SUVARTOJIMO NAUDOJANT BEVIELĘ TECHNOLOGIJĄ PROJEKTAS

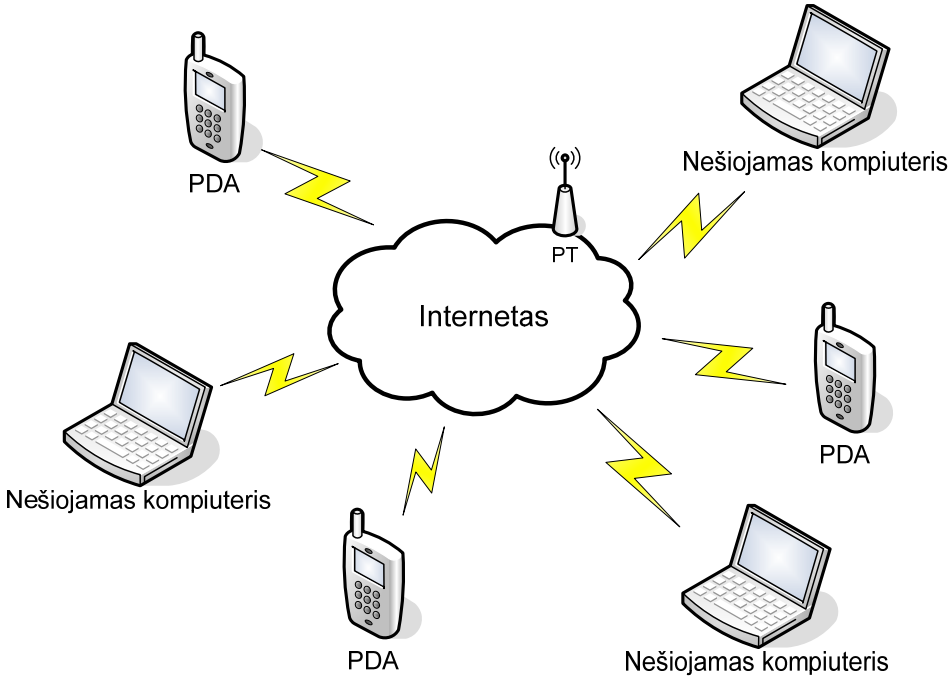
Tyrimui atlikti sukurta programinė įranga, suprogramuota C# programavimo kalba. Programinė įranga atsiunčia pasirinktus failus ir atlieka baterijos energijos matavimus. Gautus rezultatus įrašo į rezultatų failą, kuriuos išanalizavus pateikiamos išvados.

2.1 Tyrimo srities apibrėžimas

Sparčiai augant informacinėms technologijoms atsirado ir buvo pradėta naudotis skaičiavimo debesiu (angl. cloud computing), kuris atnešė naudą mokslui, verslui ir kitoms gyvenimo sritims. Jis apima tris pagrindinius komponentus: programinę įrangą, kompiuterinę įrangą ir tinklus, kurie ir sudaro „debesį “. Skaičiavimo debesyje programos, duomenys ir IT ištekliai pateikiami kaip paslauga per internetą [20] ir yra pasiekiami iš bet kurio pasaulio taško.

Atsiradus skaičiavimo debesiui, mobilus darbas tapo labai svarbus. Didelė dalis svarbios informacijos gali būti nesunkiai pasiekiama bet kuriuo metu mobiliaisiais įrenginiais prisijungus prie interneto duomenų saugyklų bevieliu ryšiu. Tolimesnis skaičiavimo debesiu paremtų paslaugų plitimas yra neišvengiamas, nes naudotojai nori būti nuolat prisijungę ir naudotis savo duomenimis visur ir visada.

8 paveiksle pavaizduotas skaičiavimo debesies modelis. Mobilūs įrenginiai – nešiojami kompiuteriai, delninukai, išmanieji telefonai, jungiasi bevieliu (Wi-Fi) ryšiu prie interneto resursų. Saugai užtikrinti naudojami analizės dalyje išanalizuoti saugos protokolai.

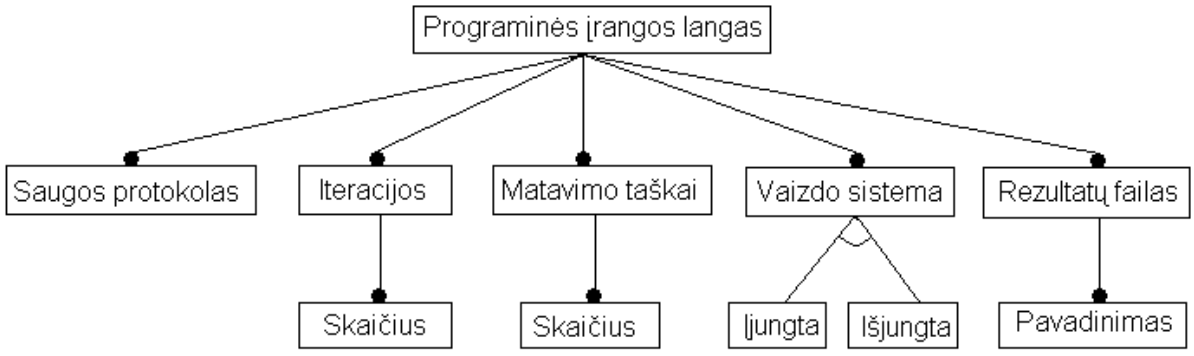


8 paveikslas. Skaičiavimo debesis

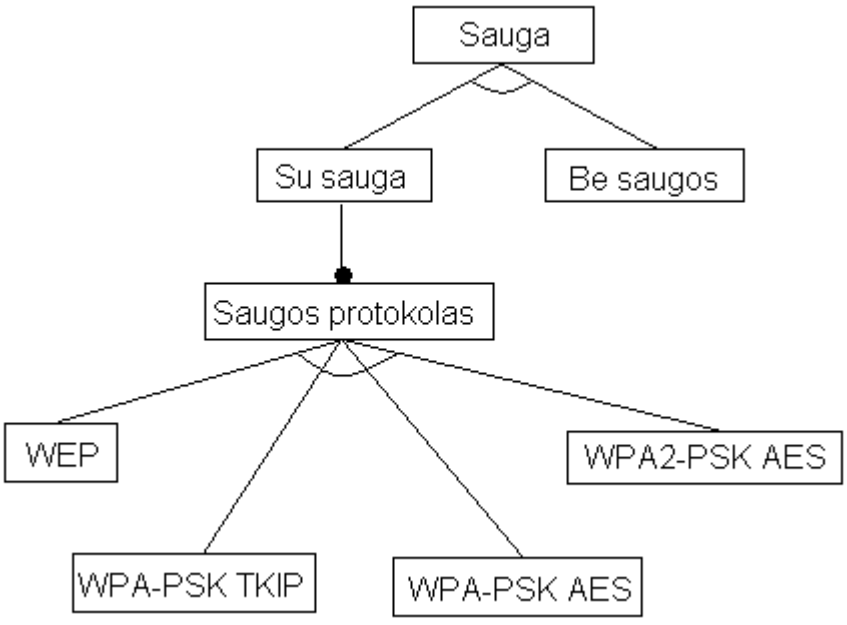
2.2 Tyrimo modelis

Tyrimo modelis pateikia tyrimo planą, kuriame aprašomi tyrimo uždaviniai, nurodomi tiriamieji ir tyrimo metodai, pagal šį nusistatytą pavyzdį yra kuriama programa [21]. Vaizdžiai tyrimo modelis pateikiamas požymių diagrama (angl. Feature diagram), kuri suteikia daug informacijos apie produkto variantiškumą. Ji palengvina sudėtingų sistemų galimybių įsisavinimą, kadangi jos tyrinėjamos aukštesniame apibendrintame lygyje, kuomet nesigilinama į kiekvieno komponento savybes ar trūkumus. Požymių diagramoje pagal nustatytus žymėjimus braižomas požymių medis, kuris atspindi galimus funkcijų pasirinkimus.

Ryšiai tarp tėvo ir vaiko požymių yra skirstomi į keturias rūšis: privalomas – vaiko požymis yra privalomas; pasirinktinai – vaiko požymis yra neprivalomas; arba – turi būti pasirinktas bent vienas iš esamų požymių; alternatyva – turi buti pasirinktas vienas požymis.



a)



b)

9 paveikslas. Požymių diagrama: a) programinės įrangos lango, b) saugos pasirinkimo.

Tyrimo uždavinys – nustatyti kiek energijos sunaudoja pasirinktas saugos protokolas. Šiam uždaviniui spręsti, pagal 9 paveiksle sudarytą požymių diagramą, sukuriamas programinis įrankis imituojantis naudotojo veiksmus. Tyrimas vykdomas pasirinkus vieną iš saugos protokolų arba be jo. Programoje turi būti galimybė pasirinkti norimą saugos protokolą: WEP, WPA-PSK TKIP, WPA-PSK AES, WPA2-PSK AES. Programinis įrankis taip pat turi turėti kitus nustatymus: iteracijų skaičiaus ir matavimo taškų pasirinkimo galimybę, vaizdo sistemos išjungimo funkciją. Turi būti galimybė išsaugoti rezultatus rezultatų faile bei pasirinkti šio failo pavadinimą.

2.3 Tyrimo metodika

Aptariant tyrimo metodiką, aprašomos visos sąlygos, kurios reikalingos norint gerai atlikti darbą.

Siuntimo – gavimo signalo maksimaliam užtikrinimui reikia sukurti atitinkamas sąlygas, todėl tyrimas atliekamas su delninuku, kuris yra padėtas nedideliu atstumu nuo serverio. Taip gauti rezultatai bus tikslesni, neįtakojami kitų trukdžių. Šiomis beveik „idealiomis sąlygomis“ gauti rezultatai parodys, kiek būtent saugos protokolas sunaudoja energijos. Tyrimo pradžioje serveryje ir delniniame kompiuteryje sukonfigūruojamas pasirinktas Wi-Fi saugos protokolas. Failas ar failų rinkinys, kuris bus siunčiamas tyrimo metu patalpinamas FTP serveryje. Programinė įranga tyrimui gali naudoti bet kokio tipo failus. Mūsų tyrime pasirenkamas etaloninis failas. Tyrėjams, kurie norės pakaroti tyrimus ar palyginti rezultatus, bus paprasčiau tai padaryti, nes etaloniniai failai yra paviešinti internete ir laisvai prieinami. Sukurtas programinis įrankis įdiegiamas į delninuką. Įėjus į šį įrankį nurodomi pradiniai veiksmai: iteracijų skaičius, matavimo taškų skaičius, pasirinkto saugos protokolo pavadinimas bei rezultatų failo pavadinimas. Prieš paleidžiant vykdyti programą, išjungiamas grafinės kortos veikimas, kurio veikimas sunaudoja daug energijos delniniame kompiuteryje, todėl gaunami rezultatai bus tikslesni. Paleidus vykdyti, atsiunčiami failai, atliekami matavimai, kurie registruojami rezultatų faile. Juos atlikus, grafinė korta vėl įjungiama ir galime pabaigti tyrimą.

Eksperimento rezultatai yra saugomi tekstiniuose failuose (*.txt). Jų pavadinimą galima nurodyti prieš pradedant tyrimą. Tai patogu, kai eksperimentų kiekis didelis. Rezultatus lengva eksportuoti į Microsoft Excel sistemą ir apdoroti. Juose įrašoma informacija apie saugos protokolus, atsiųstų failų bendras dydis, iteracijų skaičius, matavimo taškų kiekis, informacija apie baterijos būseną (akumuliatoriaus energija procentais), bei laikas po užduoto failų kiekio atsiuntimo. Pirma eilutė rezultatų faile įrašoma prieš pradedant failų siuntimą, nurodomas pradinis laikas bei su kiek pakrauta baterija pradedamas tyrimas. Ši

informacija reikalinga, norint nustatyti per kiek laiko ir kiek procentų išsikrovė baterija atlikus pirmą iteracijų ciklą.

Tyrime naudojamas iteracijos skaičius nustatomas praktiniu būdu, pagal gautus duomenis panaudojus 100 iteracijų ir gavus rezultatus.

Tyrimas atliekamas su pilnai įkrauta delninuko baterija ir vykdomas iki kol baterija pasiekia 20-30% ribą, po kurios būtų gaunami netikslūs duomenys. Po kiekvieno bandymo baterija vėl pilnai įkraunama. Bandymas atliekamas kelis kartus, tomis pačiomis sąlygomis, stebima ar rezultatai gaunami panašūs ar žymiai skiriasi.

2.4 Programos aprašymas

Programinis įrankis realizuoja failų atsisiuntimą iš serverio, naudojantis beviele Wi-Fi technologija. Vykdant programą yra fiksuojami ir registruojami duomenys apie pasirinktą iteracijų skaičių ir matavimo taškus, jų atlikimo laiką ir baterijos energijos mažėjimą procentais.

2.4.1 Panaudojimo atvejų diagrama

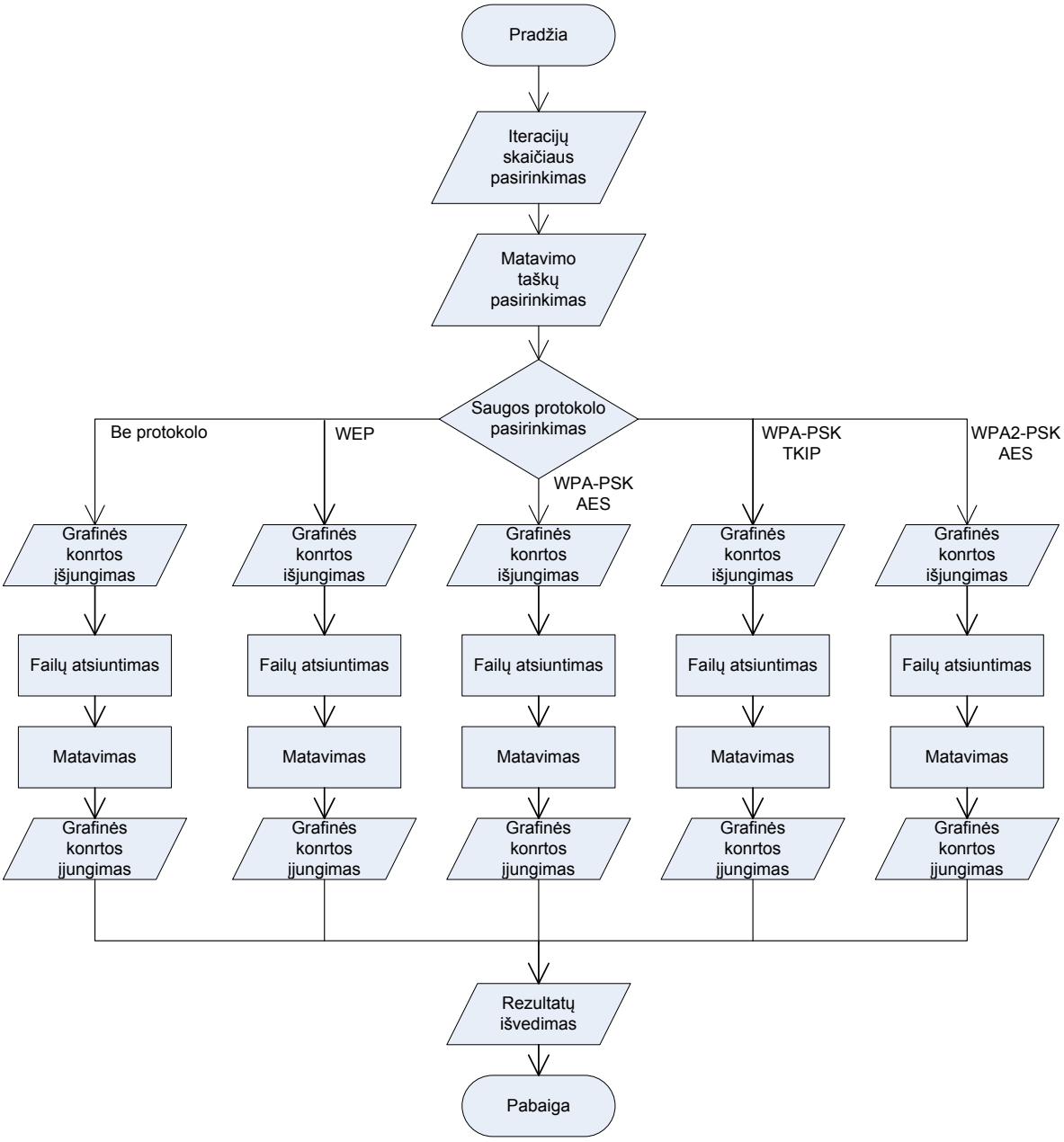
Panaudojimo atvejų diagrama pateikta 10 paveiksle. Veikiantis asmuo yra tyrėjas. Jis gali atlikti visus veiksmus su sistema. Galimos funkcijos: pasirinkti neapsaugotą Wi-Fi, WEP, WPA-PSK(AES), WPA-PSK(TKIP),WPA2-PSK(AES). Pasirinkus saugos protokolą, būtina pasirinkti matavimo taškus ir iteracijų skaičių. Rezultatų failo pasirinkimas – leidžia nurodyti norimą failo pavadinimą. Vaizdo kortos išjungimas – naudotojas gali išjungti vaizdo kortos veikimą.

10 paveikslas. Panaudojimo atvejų diagrama

2.4.2 Blokinė schema

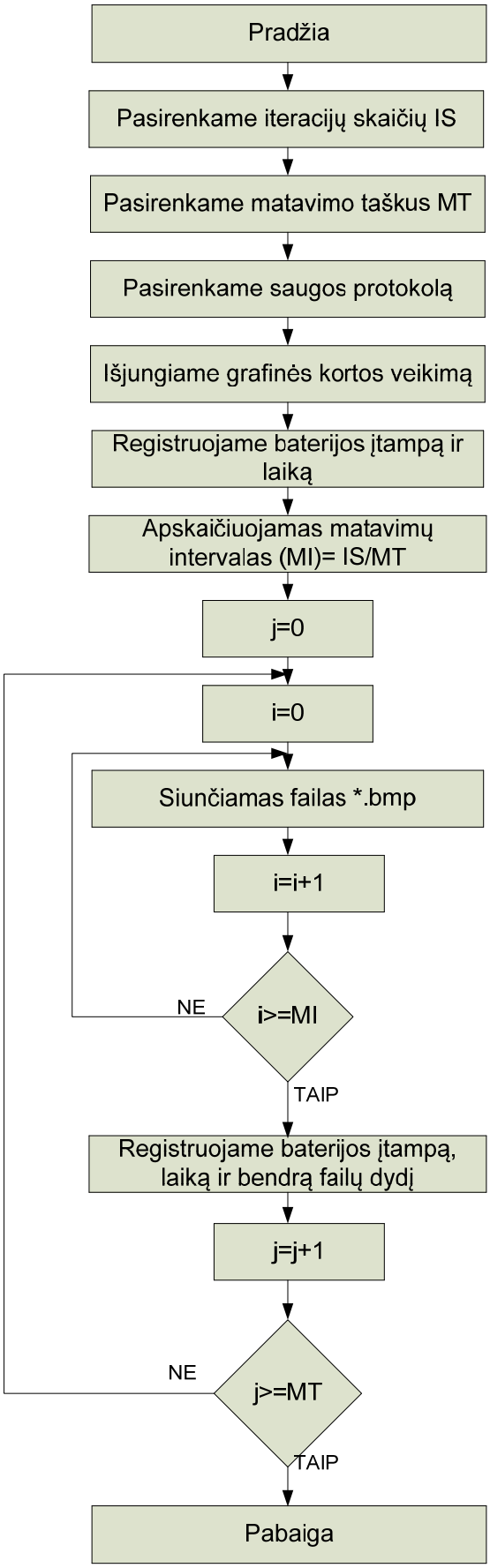
Blokinė schema yra sistemos schema, kurioje pagrindinės dalys ar funkcijos yra parodomos kaip blokai, sujungti linijomis, kurios nusako ryšius tarp jų. Apibendrinta saugos protokolo pasirinkimo blokinė schema pavaizduota 11 paveiksle. Pradžioje reikia pasirinkti iteracijų skaičių. Kadangi delninukas neturi didelės vietos duomenims saugoti, todėl įvedamas kintamasis – iteracijų skaičiaus, reikalingas, norint tyrimą atlikti su dideliu duomenų kiekiu.

Taip galima siųsti mažesnio dydžio failą pasirinktą iteracijų kiekį. Antras žingsnis yra pasirinkti matavimo taškus. Jie nurodo kiek rezultatų reikšmių norime gauti. Kiek bus pasirinkta taškų, tiek bus nuskaityta duomenų į rezultatų failą. Kuo daugiau jų pasirinkta, tuo tikslesnius grafikus bus galima pateikti apdorojus gautus duomenis. Trečias žingsnis grafinės kortos išjungimas. Tolimesni žingsniai vykdomi pasirinkus vieną iš saugos protokolų: vykdomos failo siuntimo ir matavimo funkcijos. Pabaigoje rezultatai išvedami į rezultatų failą.



11 paveikslas. Apibendrinta saugos protokolo pasirinkimo blokinė schema

Vieno saugos protokolo taikymo algoritmo blokinė schema pateikta 12 paveiksle.

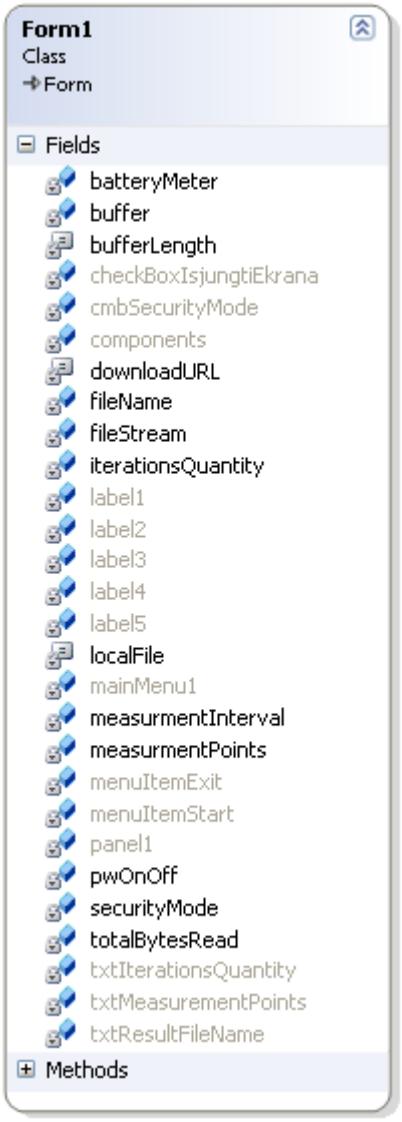


12 paveikslas. Detali saugos protokolo taikymo algoritmo blokinė schema

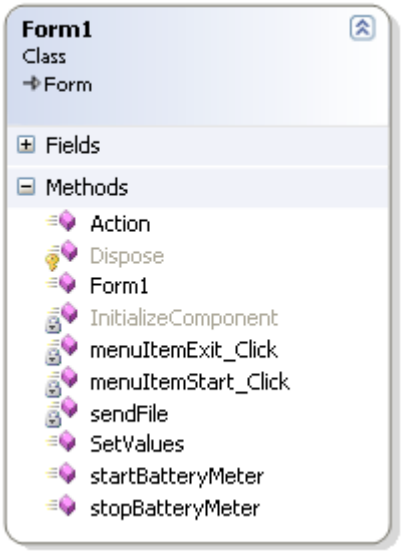
2.4.3 Naudojamos klasės aprašymas

Pasirinktas programavimo įrankis: Visual Studio 2008 Professional Edition – C# – .NET Compact Framework. Sukurta pagrindinė forma `public partial class Form1 : Form`. Joje aprašyti kintamieji ir metodai, kurie vykdo visus numatytus programos veiksmus: matuoja baterijos išsikrovimą, fiksuoja duomenis apie laiką, iteracijų kiekį, apskaičiuoja matavimo taškų intervalus, išjungia grafinės kortos veikimą, rezultatus įrašo į rezultatų failą.

Naudojamų kintamųjų sąrašas pateikiamas 13 paveiksle. Svarbus yra „iterationsQuantity“, nusakantis iteracijų skaičių. Kintamasis „measurmentPoints“ reikalingas matavimo reikšmėms gauti. Koks skaičius bus nurodytas, tiek matavimo reikšmių bus nuskaityta į rezultatų failą. Kintamasis „measurementInterval“ neįrašomas į rezultatų failą, tai tarpinis kintamasis, skirtas apskaičiuoti intervalui, kuris reikalingas atlikti tolimesniems programos veiksmams. „totalBytesRead“ naudojamas apskaičiuoti atsiųstų duomenų kiekiui.



13 paveikslas. Naudojamų kintamųjų sąrašas



14 paveikslas. Naudojamų metodų sąrašas

Programoje naudojami metodai pateikti 14 paveiksle. „Action“ metodas aprašo pagrindinius vykdomus veiksmus – baterijos matavimo paleidimą, informacijos įrašymą į log failą prieš pradedant siuntimą, failų siuntimą ir jų dydžių sumavimą, informacijos įrašymą į log failą po kiekvieno matavimo intervalo, baterijos matavimo sustabdymą. „SetValues“ nustato pagrindines reikšmes: failo pavadinimą, iteracijų skaičių, matavimo taškus, matavimų intervalą, kuris gaunamas bendrą iteracijų skaičių padalinus iš matavimo taškų, ir saugos protokolą. Failo siuntimą vykdo metodas „sentFile“. Baterijos matavimo pradėjimui naudojamas metodas „startBatteryMeter()”. Metodas „menuItemStart_Click“ aprašo programos paleidimo veiksmus. Patikrinama ar pasirinktas saugos protokolas, jei pasirinkta, išjungiamas ekrano veikimas, atliekami failų siuntimo bei baterijos matavimo veiksmai, jiem pasibaigus, vėl įjungiamas ekranas. Jei įvyko klaida, ekranas įjungiamas ir gaunamas klaidos pranešimas. Baterijos matavimo sustabdymui naudojamas metodas „stopBatteryMeter()”.

Programoje pridėta .dll biblioteka „wb.BatteryMonitor“, kuri reikalinga atlikti baterijos energijos matavimo darbams.

Programinio įrankio pagrindinis vaizdas pateiktas 1 priede.

3 DELNINIO KOMPIUTERIO ENERGIJOS SUVARTOJIMO EKSPERIMENTINIS TYRIMAS

Tyrimui naudojamas prieigos taškas D-Link AirPlus DI-524, kurio parametrai: 802.11g standartas, perdavimo greitis iki 54Mbps, veikia 2,4GHz dažnių diapazone, ir delninis kompiuteris ASUS P750, kurio parametrai: Pocket PC platforma, PXA270 520 MHz procesorius, 64 RAM atmintis, Windows Mobile 6 Professional operacinė sistema, 1.3 baterijos versija.

3.1 Eksperimento atlikimas

Eksperimentas atliekamas su etaloniniu failu – lena3.tif, kuris atsisiųstas iš svetainės <http://links.uwaterloo.ca/Repository.html>. Pasirinktas grafinio vaizdo failo formatas – bmp. Šio failo dydis – 786,486 baitai [22]. Kompiuteryje naudojama Microsoft sistema, todėl įdiegta interneto informacijos sistema (angl. Internet information services, IIS), kuri palaiko FTP paslaugas. FTP serveris naudojamas įkelti ir atsisiųsti failams. Etaloninis failas patalpinamas šiame serveryje ir paviešinamas. Delniniame kompiuteryje patalpinama tyrimui sukurta programa. Joje nurodomas kelias kur yra patalpintas atsisiuntimui skirtas etaloninis failas. Prieigos taškas ir delninis kompiuteris sukonfigūruojami prieš kiekvieną tyrimą. Šios konfigūracijos pateiktos 6 ir 7 lentelėse. Eksperimento metu delninio kompiuterio ekranas išjungiamas. Pasibaigus tyrimui, rezultatai įrašomi į tekstinį failą, po to perkeliami į stacionarų kompiuterį ir apdorojami.

Prieigos taškas bei delninukas turėjo nustatymuose pasirinkimą WPA-PSK AES. Todėl bandymą buvo galima atlikti ir su šiuo pasirinkimu. Tačiau ne kiekvienas prieigos taškas turi galimybę pasirinkti šį saugos nustatymą. Tinklo raktas buvo pasirinktas dešimties simbolių slaptažodis, sudarytas iš skaičių ir raidžių. Autentifikavimui naudojamas padalintų raktų metodas (PSK).

6 lentelė. Eksperimentui atlikti naudotų prieigos taško bevielio tinklo konfigūracijos nustatymų sąrašas

Saugos protokolas	Duomenų šifravimo algoritmas	Tinklo raktas
Be protokolo	–	–
WEP	128Bit	10 simbolių
WPA-PSK	AES	10 simbolių
WPA-PSK	TKIP	10 simbolių
WPA2-PSK	AES	10 simbolių

7 lentelė. Eksperimentui atlikti naudotų PDA bevielio tinklo konfigūracijos nustatymų sąrašas

Saugos protokolas	Duomenų šifravimo algoritmas	Tinklo raktas
Be protokolo	–	–
WEP	Open	10 simbolių
WPA-PSK	AES	10 simbolių
WPA-PSK	TKIP	10 simbolių
WPA2-PSK	AES	10 simbolių

Tyrimo rezultatų failas sudarytas iš 8 lentelėje nurodytų laukų. Taip lengviau ir greičiau galima apdoroti gautus duomenis.

8 lentelė. Rezultatų failo laukų aprašymas

Eil.Nr.	Lauko pavadinimas	Lauko aprašymas
1.	Securitymode	Pasirinktas saugos protokolas (-,WEP,WPA–PSK (AES), WPA-PSK (TKIP), WPA2-PSK (AES))
2.	IterationsQuantity	Iteracijų kiekis
3.	MeasurmentPoints	Matavimo taškai, nurodantys kiek matavimų reikšmių bus nuskaityta į rezultatų failą
4.	BytesSend	Atsiųstų baitų kiekis
5.	Date	Tyrimo atlikimo data metai:mėnuo:diena
6.	Time	Laikas, per kurį įvykdytas vienas siuntimo ciklas
7.	BatteryLifePercentage	Baterijos energija procentais

Kiekvienas bandymas, pasirinkus konkretų saugos protokolą ir kitus duomenis, įrašomas į atskirą *.txt failą. Bandymo rezultatų failo pavyzdys pateiktas 15 paveiksle.

```
SecurityMode;IterationsQuantity;MeasurmentPoints;BytesSend;Date;Time;
WPA-PSK(TKIP);0;0;0;10.12.16;10:53:16; 99;
WPA-PSK(TKIP);350;1;275270100;10.12.16;11:02:00; 90;
WPA-PSK(TKIP);700;2;550540200;10.12.16;11:10:49; 82;
WPA-PSK(TKIP);1050;3;825810300;10.12.16;11:19:39; 74;
WPA-PSK(TKIP);1400;4;1101080400;10.12.16;11:28:29; 67;
WPA-PSK(TKIP);1750;5;1376350500;10.12.16;11:37:17; 59;
WPA-PSK(TKIP);2100;6;1651620600;10.12.16;11:46:04; 51;
WPA-PSK(TKIP);2450;7;1926890700;10.12.16;11:54:56; 44;
WPA-PSK(TKIP);2800;8;2202160800;10.12.16;12:03:43; 37;
WPA-PSK(TKIP);3150;9;2477430900;10.12.16;12:12:32; 30;
WPA-PSK(TKIP);3500;10;2752701000;10.12.16;12:21:19; 23;
```

15 paveikslas. Bandymo rezultatų failo pavyzdys

3.2 Eksperimento rezultatai

Atlikus eksperimentą, gauti tyrimo rezultatai pateikiami 9–14 lentelėse.

9 lentelė. Tyrimo duomenys, neapsaugotas Wi-Fi

Saugos protokolas	Baterijos likutis, viso %	Iteracijų kiekis	Atsisiųstų duomenų kiekis, MB	Apdorojimo laikas, viso HH:MM:SS	Baterijos pokytis, %
–	99	0	0	00:00:00	0
	92	500	375,03	00:08:55	7
	86	1000	750,05	00:17:54	6
	79	1500	1125,08	00:26:55	7
	72	2000	1500,10	00:35:52	7
	66	2500	1875,13	00:44:49	6
	59	3000	2250,15	00:53:56	7
	52	3500	2625,18	01:02:52	7
	46	4000	3000,21	01:11:50	6
	40	4500	3375,23	01:20:48	6
	34	5000	3750,26	01:29:46	6

10 lentelė. Tyrimo duomenys, WEP protokolas

Saugos protokolas	Baterijos likutis, viso %	Iteracijų kiekis	Atsisiųstų duomenų kiekis, MB	Apdorojimo laikas, viso HH:MM:SS	Baterijos pokytis, %
WEP	99	0	0	00:00:00	0
	92	500	375,03	00:08:44	7
	86	1000	750,05	00:17:32	6
	78	1500	1125,08	00:26:20	8
	72	2000	1500,10	00:35:09	6
	64	2500	1875,13	00:44:00	8
	58	3000	2250,15	00:52:50	6
	51	3500	2625,18	01:01:39	7
	44	4000	3000,21	01:10:31	7
	38	4500	3375,23	01:19:24	6
	31	5000	3750,26	01:28:18	7

11 lentelė. Tyrimo duomenys, WPA-PSK (AES) protokolas

Saugos protokolas	Baterijos likutis, viso %	Iteracijų kiekis	Atsisiųstų duomenų kiekis, MB	Apdorojimo laikas, viso HH:MM:SS	Baterijos pokytis, %
WPA-PSK AES	99	0	0	00:00:00	0
	92	500	375,03	00:09:18	7
	84	1000	750,05	00:18:38	8
	77	1500	1125,08	00:27:57	7
	69	2000	1500,10	00:37:17	8
	60	2500	1875,13	00:46:37	9
	52	3000	2250,15	00:55:55	8
	45	3500	2625,18	01:05:11	7
	37	4000	3000,21	01:14:32	8
	30	4500	3375,23	01:23:54	7
	22	5000	3750,26	01:33:14	8

12 lentelė. Tyrimo duomenys, WPA2-PSK (AES) protokolas

Saugos protokolas	Baterijos likutis, viso %	Iteracijų kiekis	Atsisiųstų duomenų kiekis, MB	Apdorojimo laikas, viso HH:MM:SS	Baterijos pokytis, %
WPA2-PSK AES	100	0	0	00:00:00	0
	92	500	375,03	00:09:16	8
	83	1000	750,05	00:18:38	9
	74	1500	1125,08	00:30:58	9
	66	2000	1500,10	00:40:28	8
	58	2500	1875,13	00:49:46	8
	50	3000	2250,15	00:59:05	8
	42	3500	2625,18	01:08:26	8
	34	4000	3000,21	01:17:47	8
	27	4500	3375,23	01:27:07	7
	20	5000	3750,26	01:36:29	7

13 lentelė. Tyrimo duomenys, WPA-PSK (TKIP) protokolas

Saugos protokolas	Baterijos likutis, viso %	Iteracijų kiekis	Atsisiųstų duomenų kiekis, MB	Apdorojimo laikas, viso HH:MM:SS	Baterijos pokytis, %
WPA-PSK TKIP	99	0	0	00:00:00	0
	90	350	262,52	00:08:44	9
	82	700	525,04	00:17:33	8
	74	1050	787,55	00:26:23	8
	67	1400	1050,07	00:35:13	7
	59	1750	1312,59	00:44:01	8
	51	2100	1575,11	00:52:48	8
	44	2450	1837,63	01:01:40	7
	37	2800	2100,14	01:10:27	7
	30	3150	2362,66	01:19:16	7
	23	3500	2625,18	01:28:03	7

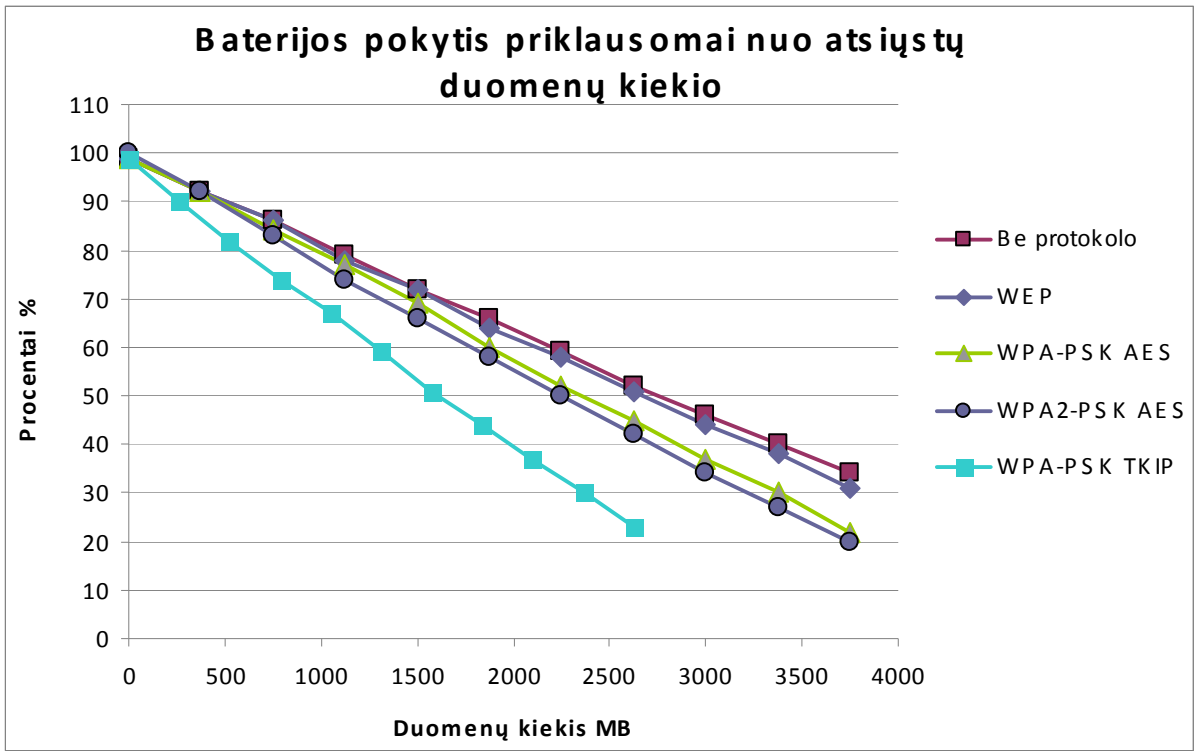
14 lentelė. Apibendrinti eksperimento rezultatai

Nr.	Saugos protokolas	Bendras apdorojimo laikas	Baterijos pokytis %	Atsisiųstų duomenų kiekis MB
1.	–	01:29:46	65%	3750
2.	WEP	01:28:18	68%	3750
3.	WPA-PSK AES	01:33:14	77%	3750
4.	WPA2-PSK AES	01:36:29	80%	3750
5.	WPA-PSK TKIP	01:28:03	76%	2625

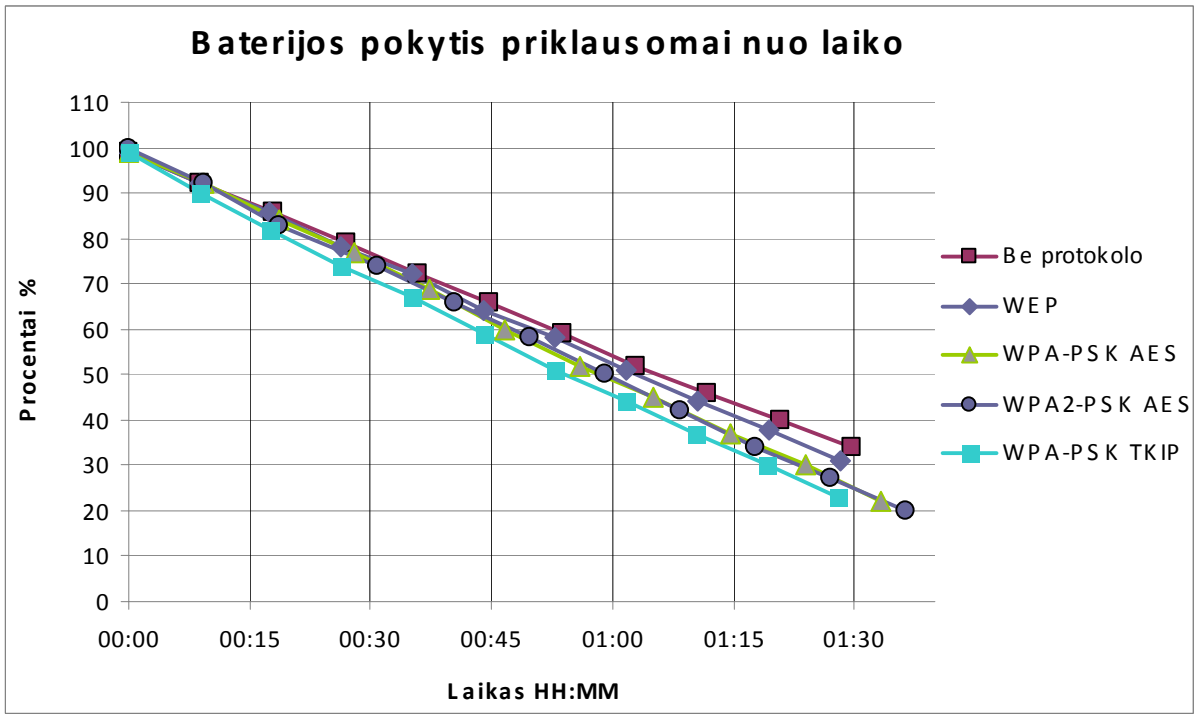
Kad galėtume palyginti naudotus saugos protokolus, iš gautų rezultatų brėžiame grafikus.

Iš gautų rezultatų (16-17 paveikslai) matome, kad siunčiant duomenis daugiausiai energijos sunaudota WPA-PSK TKIP saugos protokolas. Atsisiųstas duomenų kiekis žymiai mažesnis, nei naudojant kitus protokolus. Nepanaudojus protokolo ir panaudojus WPA-PSK AES taip pat susidaro 12% skirtumas. Tarp visų protokolų matomas kelių procentų skirtumas.

Iš laiko grafiko matome, kad WPA2 ir WPA-PSK AES protokolai užtruko ilgiau laiko atsiųsti tam pačiam duomenų kiekiui, nei pasirinkus WEP protokolą.



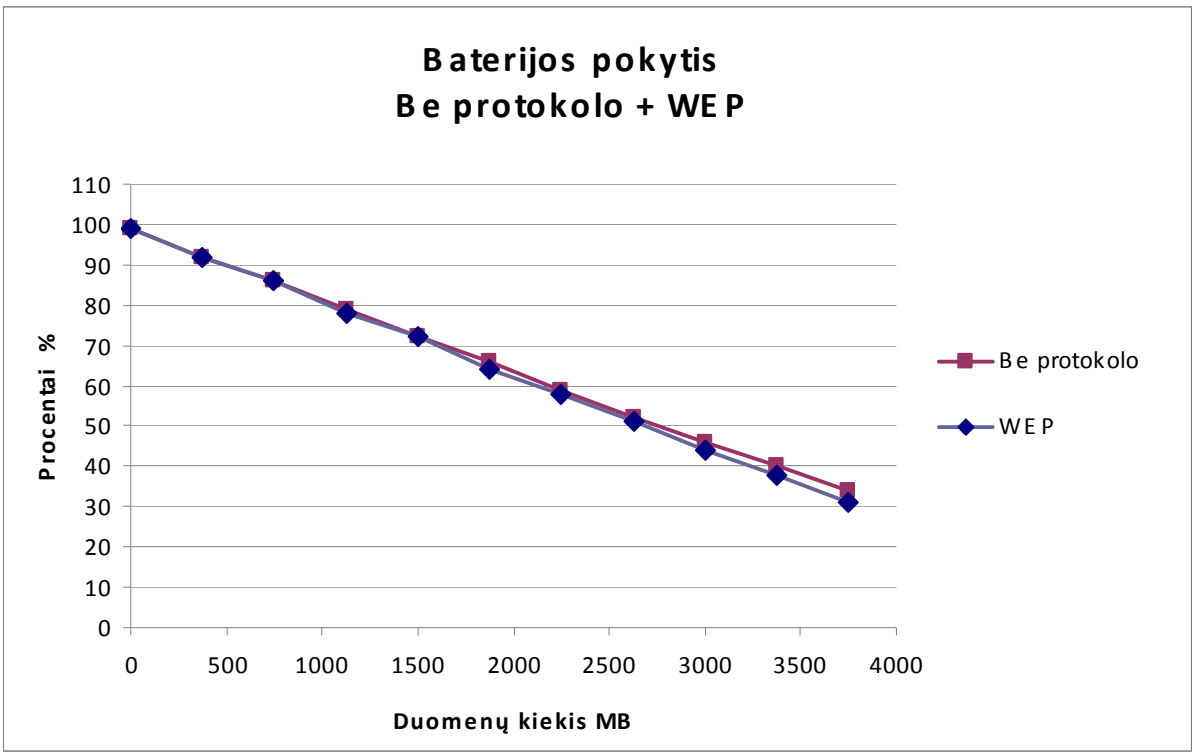
16 paveikslas. Baterijos pokytis pagal duomenų kiekį



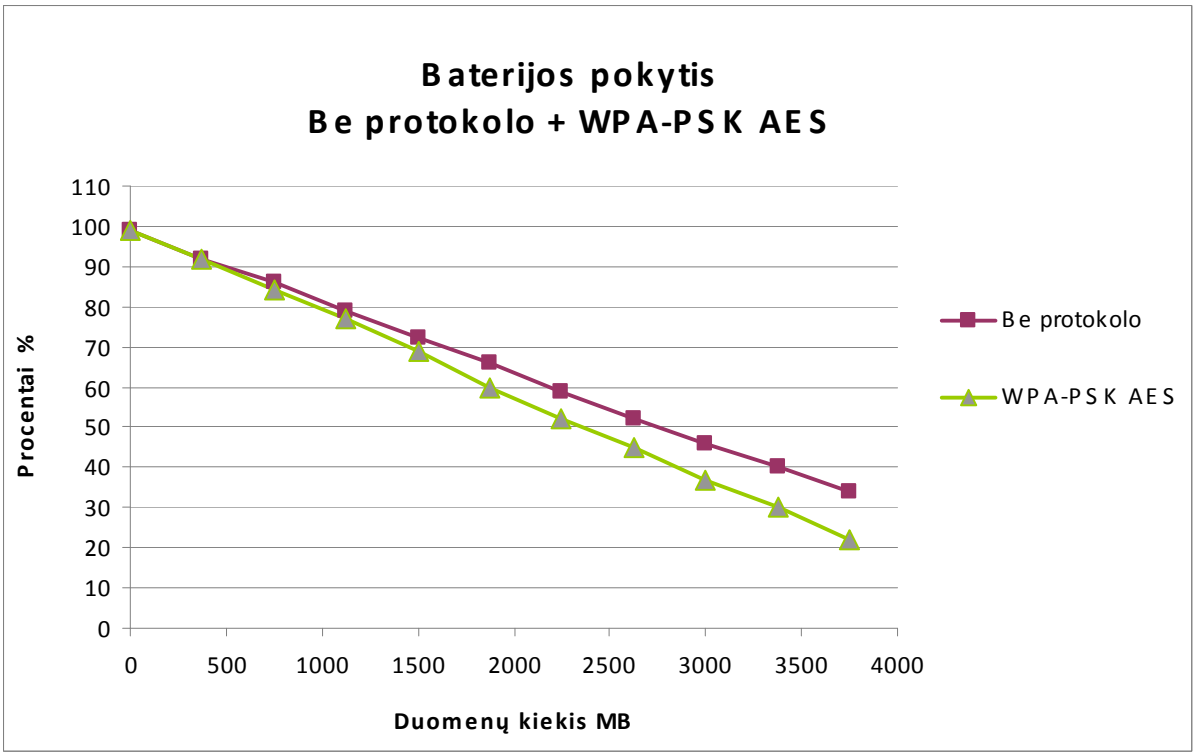
17 paveikslas. Baterijos pokytis pagal laiką

Atlikus eksperimentą, be saugos protokolo ir su juo, gaunamas suvartotos energijos skirtumas (1). Taip galime nustatyti kiek procentų sunaudoja kiekvienas protokolas atskirai (18-21 paveikslai).

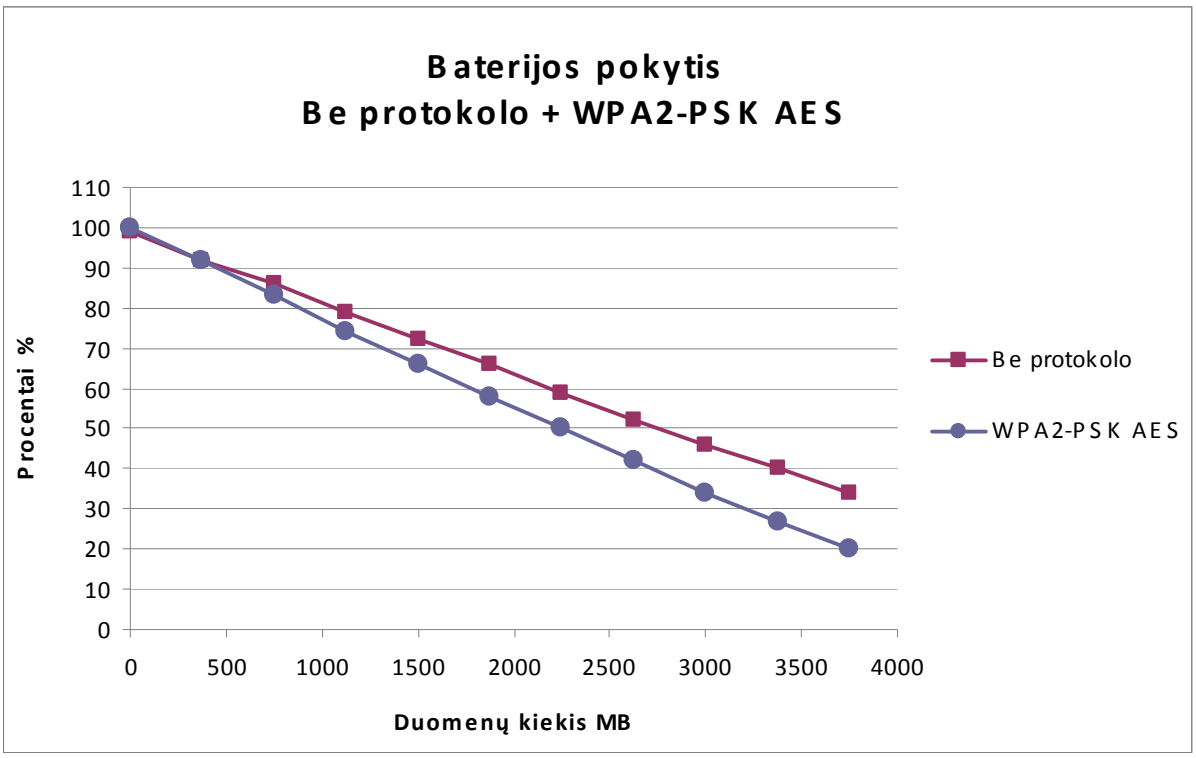
Be saugos protokolo(BSP) – Su saugos protokolu(SSP) = energijos skirtumas. (1)



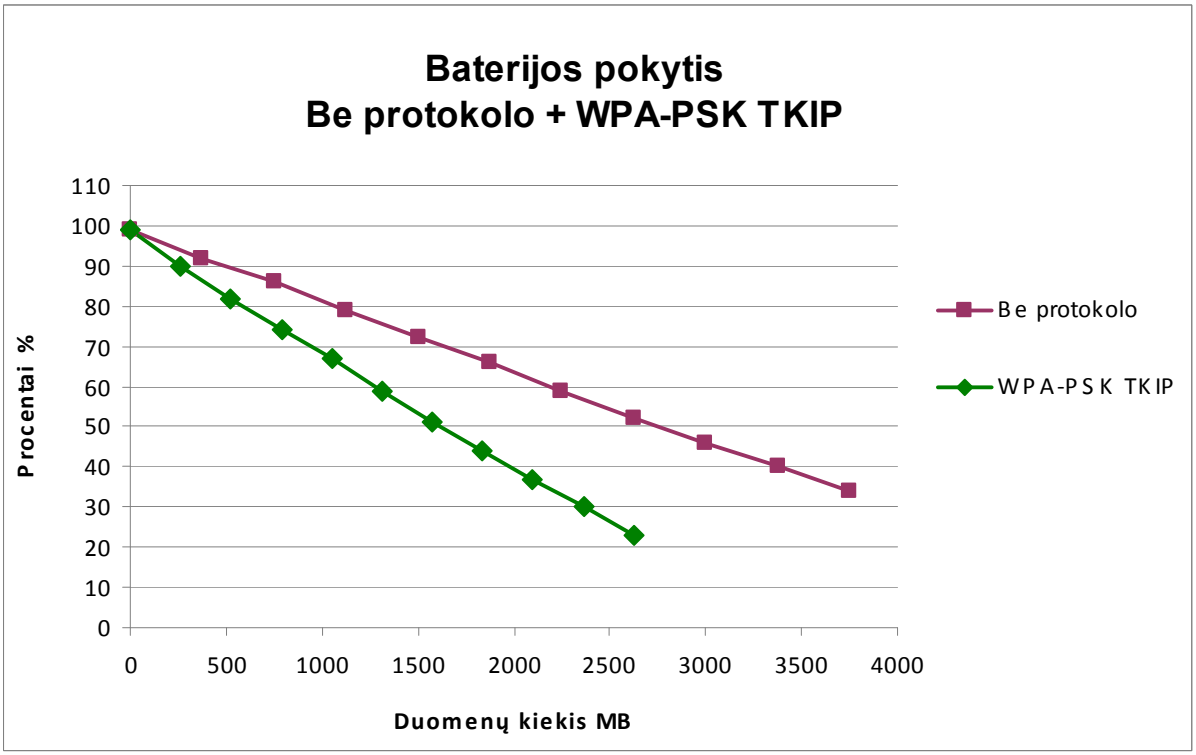
18 paveikslas.Be protokolo – WEP. Baterijos pokytis pagal duomenų kiekį



19 paveikslas. Be protokolo – WPA-PSK AES. Baterijos pokytis pagal duomenų kiekį



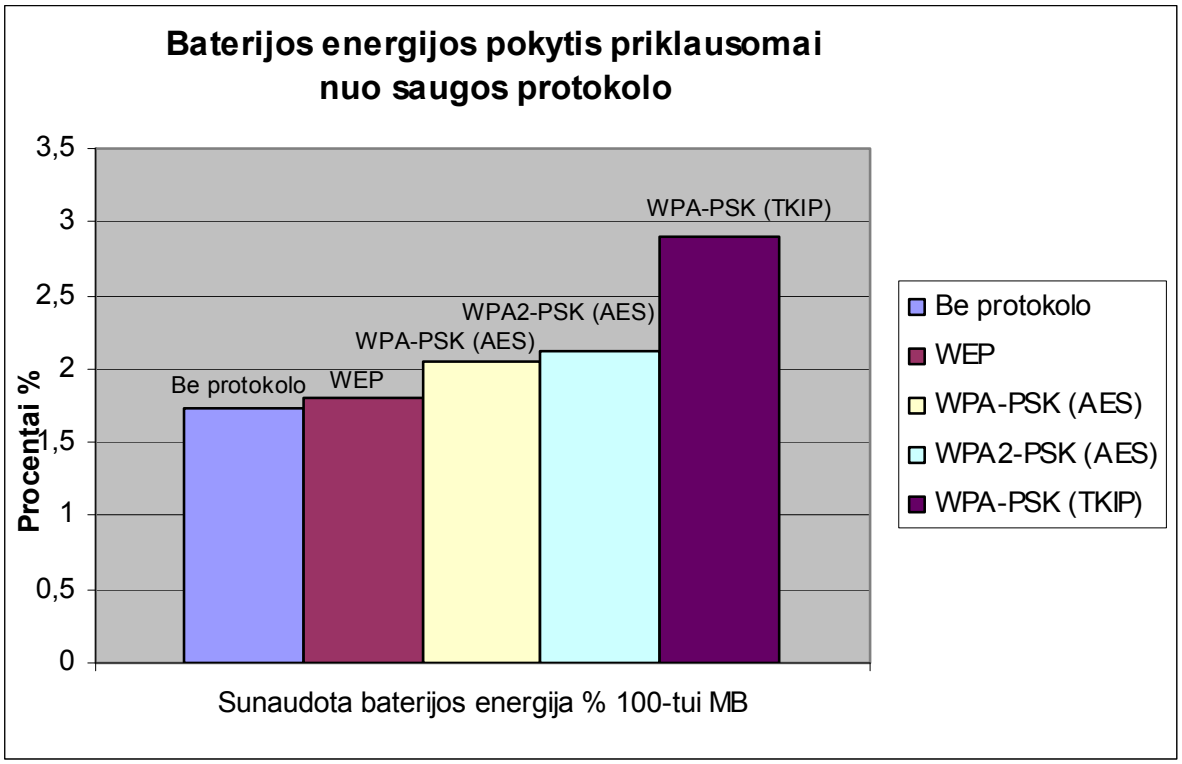
20 paveikslas. Be protokolo – WPA2-PSK AES. Baterijos pokytis pagal duomenų kiekį



21 paveikslas. Be protokolo – WPA-PSK TKIP. Baterijos pokytis pagal duomenų kiekį

Kadangi ne visiems tyrimams iteracijų skaičius buvo vienodas, gautų rezultatų apibendrinimui pateikiamas detalesnis grafikas (22 paveikslas), kuriame apskaičiuota kiek sunaudota energijos šimto megabaitų duomenų atsisiuntimui panaudojus pasirinktą saugos protokolą. Pastebime, kad nenaudojant protokolo ir pasirinkus WEP, WPA – PSK (AES) ar

WPA2 – PSK (AES), rezultatai gaunami panašūs, atitinkamai (1,73%, 1,81%, 2,05%, 2,13%). Tačiau palyginus su WPA – PSK (TKIP) skiriasi daugiausiai (2,9%).



22 paveikslas. Baterijos sunaudota energija % 100tui MB

3.3 Eksperimento išvados

- Sudaryta tyrimo metodika, pagal kurią atliktas eksperimentas ir gauti rezultatai, nurodantys energijos suvartojimą pagal pasirinktą Wi-Fi saugos protokolą. Tyrimas patvirtino hipotezę, kad nenaudojant saugos protokolo, arba naudojant silpniausią WEP, energijos sąnaudos mažesnės, nei pasirinkus kitus protokolus (WPA –PSK, WPA2 –PSK).
- WEP palyginus su WPA-PSK (TKIP), sunaudojama trečdaliu mažiau energijos, tačiau jų saugos lygis skiriasi.
- Rezultatai, naudojant WEP saugos protokolą, ir nenaudojant jokio, skyrėsi nežymiai (68%, 65%), todėl galime patarti siunčiant duomenis bevieliu tinklu tarp PDA ir kompiuterio naudoti bent WEP saugos protokolą. Norint stipriau apsaugoti duomenis, galima rinktis WPA-PSK(AES), WPA2-PSK(AES), WPA-PSK(TKIP), kurie šimto megabaitų duomenų atsiuntimui sunaudoja atitinkamai (2,05%, 2,13%, 2,9%,) energijos.

- Apskaičiavus, kiek baterija sunaudoja energijos 100MB duomenų, tarp WPA2-PSK(AES) ir WPA-PSK(AES) gautas 0,08% skirtumas. Tarp WPA2-PSK(AES) ir WPA-PSK(TKIP) gautas 0,77% skirtumas.
- Rezultatai parodė, kad WPA-PSK(TKIP) saugos protokolo pasirinkimas nėra geriausias sprendimas, nes jis sunaudoja daugiausiai energijos ir yra pažeidžiamas.
- Turint tyrimo rezultatus, naudotojas gali pats pasirinkti saugos protokolą, įvertinant siunčiamos informacijos saugumo poreikį ir esamą delninio kompiuterio baterijos energijos likutį. Saugumo atžvilgiu (2-5 lentelės) ir sunaudotos energijos kiekiu (22pav.), mes rekomenduotume pasirinkti WPA-PSK(AES) saugos protokolą. Jeigu prieigos taškas neturi tokio nustatymo, o leidžiamas pasirinkimas tik WPA-PSK su TKIP, tokiu atveju reikėtų rinktis WPA2-PSK(AES).
- Ateityje, pratęsiant tyrimą, būtų galima ištirti kaip Wi-Fi įtakoja energijos suvartojimą, jei saugiam naudotojų ir tinklų autentifikavimui pasirenkamas 802.1X protokolas (reikalingas autentifikavimo serveris), bei naudojant saugumo sertifikatus.

4 DARBO IŠVADOS

- Atsiradus skaičiavimo debesiui, paplito mobilus darbas.
- Pagal „International Data Corp“ duomenis paskutinį 2010 metų ketvirtį išmaniųjų telefonų rinkai buvo pateikta 101 mln. (87% augimas, lyginant su atitinkamu prieš tai buvusių metų laikotarpiu).
- Išmaniuosiuose telefonuose bevielė technologija suvartoja apie 50% baterijos energijos.
- Informacijos saugą, informaciją perduodant bevieliu ryšiu, užtikrina saugos protokolai: WEP, WPA, WPA2. Jie išanalizuoti ir pateikti analizės dalyje.
- Aprašyti energijos taupymo metodai, kurie sumažina energijos suvartojimą veikiant bevielei technologijai.
- Sudarytas delninių kompiuterių energijos suvartojimo naudojant bevielę technologiją projektas, pagal kurį sukurtas programinis įrankis.
- Pateikta tyrimo metodika, pagal kurią atliktas tyrimas ir gauti rezultatai.
- Apskaičiavus, kiek baterija sunaudoja energijos 100MB duomenų, tarp WPA2-PSK(AES) ir WPA-PSK(AES) gautas 0,08% skirtumas. Tarp WPA2-PSK(AES) ir WPA-PSK(TKIP) gautas 0,77% skirtumas.
- Iš gautų tyrimo rezultatų, nustatyta, kad WPA-PSK(TKIP) saugos protokolo pasirinkimas nėra geriausias sprendimas, nes jis sunaudoja daugiausiai energijos ir yra pažeidžiamas.
- Rekomenduojama pasirinkti WPA2-PSK(AES) saugos protokolą, arba jei yra galimybė WPA-PSK(AES).
- Žinant 100MB duomenų siuntimui sunaudotą energijos kiekį, galima sužinoti kiek energijos suvartojama bet kuriam norimam duomenų kiekiui siųstis.
- Ateityje, pratęsiant tyrimą, būtų galima ištirti kaip Wi-Fi įtakoja energijos suvartojimą, jei saugiam naudotojų ir tinklų autentifikavimui pasirenkamas 802.1X protokolas (reikalingas autentifikavimo serveris), bei naudojant saugumo sertifikatus.
- Magistrinio darbo tematika parašytas straipsnis išspausdintas leidinyje „Informacinės technologijos. XVI tarpuniversitetinė magistrantų ir doktorantų konferencija.“ Straipsnis pateiktas 2 priede.
- Šia tema pristatytas pranešimas XVI tarpuniversitetinėje magistrantų ir doktorantų konferencijoje, vykusioje 2011-04-22 Kaune.

LITERATŪRA

1. J.Adams “Adaptive Buffer Power Save Mechanism for Mobile Multimedia Streaming”. *Presented for the degree of Masters in Engineering to the School of Electronic Engineering Facullty of Computing and Engineering Dublin City University Ireland,* p.114, 2007.
2. G.Anastasi, M.Conti, E.Gregori, A.Passarella. “802.11 power-saving mode for mobile computing in Wi-Fi hotspots: Limitations, enhancements and open issues”. Kluwer Academic Publishers, *Wireless Networks,* Volume 14, Issue 6, p. 745-768, 2008.
3. Y.Wei, S.Chandra, S.Bhandarkar. “A Statistical Prediction-based Scheme for Energy-aware Multimedia Data Streaming”. *Proc. In Wireless Communications and Networking Conference, 2004. WCNC. 2004 IE*, p. 2053 - 2057, 2004.
4. “How wi-fi works”. [Žiūrėta 2010-10-07]. Prieiga per internetą: <http://nostarch.com/download/wifi_01.pdf>
5. E.Shih, P.Bahl, M.J.Sinclair “Wake on Wireless: An Event Driven Energy Saving Strategy for Battery Operated Devices”. *Proc. in MobiCom '02: Proceedings of the 8th annual international conference on Mobile computing and networking*, p.160-171, 2002.
6. A.B.Lago, I.Larizgoitia.“An application-aware approach to efficient power management in Mobile Devices”. *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE*, article No: 11, 2009.
7. D.Tudor, M.Marcu. “Designing a Power Efficiency Framework for Battery Powered Systems”. *Source: ACM International Conference Proceeding Series, Proceedings of SYSTOR 2009: The Israeli Experimental Systems Conference*, article No: 5, 2009.
8. H. I. Bulbul, I. Batmaz, M. Ozel. “Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols”. *Proc. of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, Article No. 9, 2008.
9. P.Keeratiwintakorna, P.Krishnamurthyb. “An energy efficient security protocol for IEEE 802.11 WLANs”, *Pervasive and Mobile Computing*, *Volume 2, Issue 2*, p. 204-231, April 2006.
10. A.Marc, Z.Vireda, L.S.Brakmo, W.R. Hamburger. “Energy management on HandHeld Devices”. *Hewlett Packard Laboratories,* 2003.

11. N.R Potlapally, and A.Raghunathan. “A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols”. *Mobile Computing, IEEE Transactions on Volume 5, Issue 2,* p. 128-143, Feb.2006.

12. A.Rahmati, L.Zhong. “Context-for-Wireless:Context-Sensitive Energy-Efficient Wireless Data Transfer”. *Proc. ACM/USENIX Int. Conf. Mobile Systems, Applications, and Services (MobiSys)*, 2007.

13. P.Trimintzios, G.Georgiou „WiFi and WiMAX Secure Deployments“. *Hindawi Publishing Corporation. Journal of Computer Systems, Networks and Communications,* 2010.

14. Wi-Fi Alliance. „Deploying Wi-Fi Protected Access (WPA ™) and WPA2 ™ in the Enterprise“, March 2005.

15. A.B.Lashkari, M.M.S.Danesh, B.Samadi. „A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)“. *2009 2nd IEEE International Conference on Computer Science and Information Technology,* 2009.

16. A.Moscaritolo, „Vulnerability discovered in WPA encryption“, 2008.
[Žiūrėta 2011-03-27]. Prieiga per internetą:
<http://www.securecomputing.net.au/News/127719,vulnerability-discovered-in-wpa-encryption.aspx>.

17. KezNews forum. „WPA Encryption No Longer Secure“, 2008.
[Žiūrėta 2011-03-27]. Prieiga per internetą:
<http://keznews.com/5041_WPA_Encryption_No_Longer_Secure>.

18. J. Toldinas, V.Štuikys, R. Damaševičius, G.Ziberkas. „Mobiliųjų įtaisų energijos naudojimo taikomojo lygmens modeliai“. *Elektronika ir elektrotechnika. Kaunas: Technologija, 2009. Nr.6(96).* p. 73-76.

19. J. Toldinas, V.Štuikys, G.Ziberkas, D. Naunikas. „Energijos suvartojimo kriptografijos paslaugos algoritmams eksperimentas“. *Elektronika ir elektrotechnika. Kaunas: Technologija, 2010. Nr.5(101).* p. 57-62.

20. V.Rėkus. IBM pranešimas. „Naujos technologijos ir veiklos tęstinumas: būkite pasiruošę netikėtumams“, 2010.
[Žiūrėta 2011-04-18]. Prieiga per internetą:
<http://www-05.ibm.com/lt/ibmforum/pdf/naujos_technologijos_ir_veiklos_testinumas_-_bukite_pasiruose_netiketumams.pdf>.

21. Terminai. Tarptautinių žodžių žodynas.

[Žiūrėta 2011-03-01]. Prieiga per internetą:
<http://www.terminai.lt>

22. Etaloninis failas.
[Žiūrėta 2010-03-01]. Prieiga per internetą:
<http://www.researchandtechnology.net/pcif/waterloo_benchmarks.php>.

23. M. Meeker „Mobile Inernet Will Soon owertake Fixed Internet“, 2010.
[Žiūrėta 2010-12-14]. Prieiga per internetą:
<http://gigaom.com/2010/04/12/mary-meeker-mobile-internet-will-soon-overtake-fixed-internet/>.

24. J. Menn. „Smartphone shipments surpass PCs“, 2011.
[Žiūrėta 2011-03-17]. Prieiga per internetą:
<http://www.ft.com/intl/cms/s/2/d96e3bd8-33ca-11e0-b1ed-00144feabdc0.html#axzz1NLtI0jJr>.

25. IT technologijų pasaulis. „Wi-Fi technologija sparčiai populiarėja “, 2009.
[Žiūrėta 2011-05-14]. Prieiga per internetą:
<http://technologijos.eu/internetas/wi-fi-technologija-sparciai-populiareja/>.

26. Mobium.lt „Išmaniųjų telefonų baterijų veikimo laiko palyginimas“. *Publikacija elektronikos, informacijų ir ryšių technologijų portale Ekeltronika.lt,* 2010, lapkritis.
[Žiūrėta 2011-05-13]. Prieiga per internetą:
<http://www.elektronika.lt/produktai/telefonai/25913/ismaniuju-telefonu-bateriju-veikimo-laiko-palyginimas/>.

Research on pocket PCs wireless security protocols

SUMMARY

Wireless network infrastructure is based on the Wi-Fi technology, which allows access to reliable and high-speed Internet connection wirelessly. Wi-Fi network can be used in Pocket PCs (called PDAs) to connect to a computer network with the equipped access point (access point). This connection provides a secure medium for the transmission of information when using wireless network security technologies, WPA or WPA2. WEP is an older network security method and it is not secure. Merger over Wi-Fi handheld interface influences energy consumption. This work focuses on the pda's battery power consumption, depending on the selected security protocol. Provided energy-saving mode for mobile devices, security protocols are discussed. The energy assessment method and the experiment methodology are described. Based on the results, the conclusions about the choice of security protocols are done.

PRIEDAI

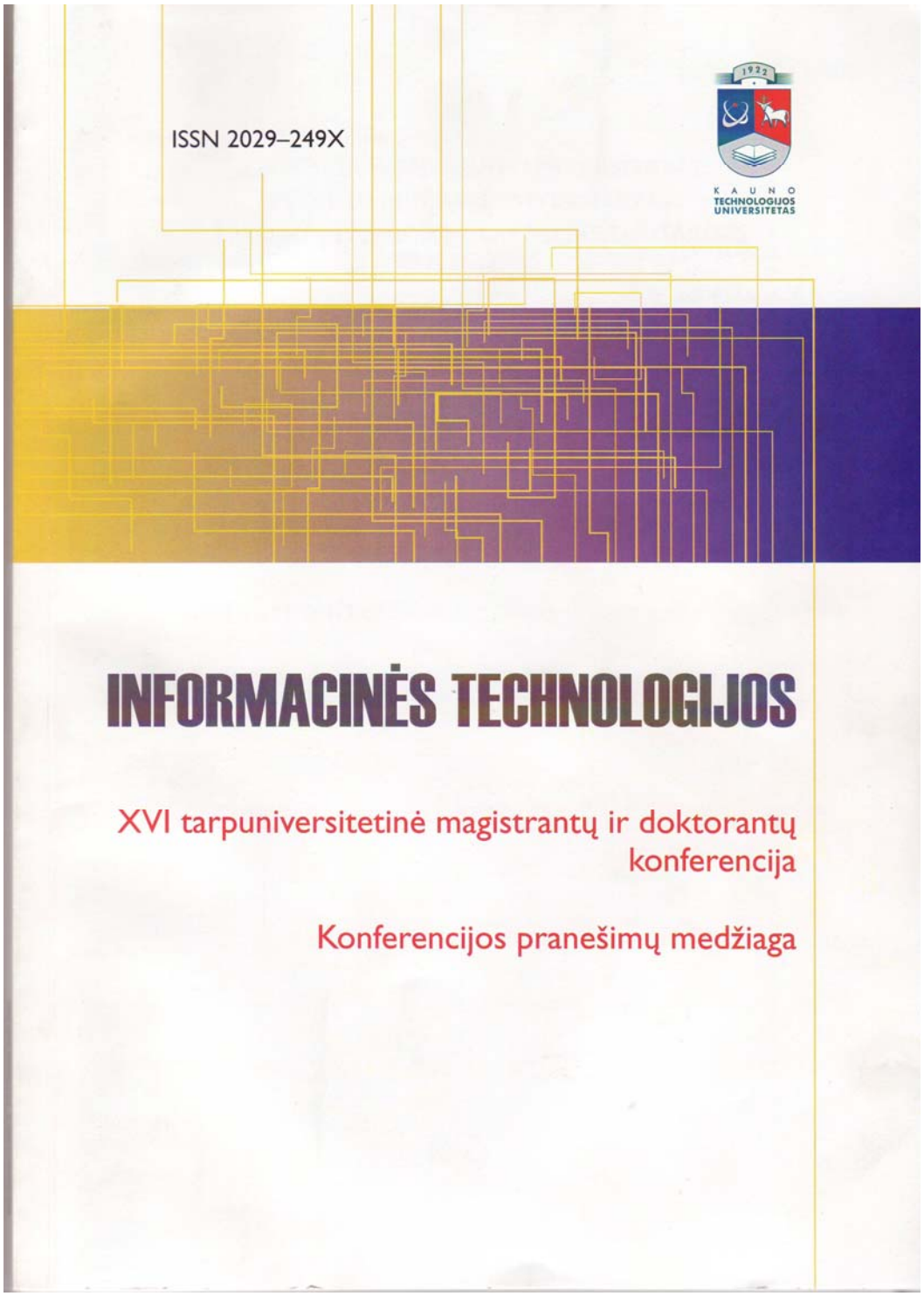
1 PRIEDAS

Programinio įrankio pagrindinis vaizdas

2 PRIEDAS

Publikacija „Wi-Fi saugos protokolų įtaka energijos suvartojimui delniniuose kompiuteriuose“

Pateikiamas mokslinis straipsnis išspausdintas leidinyje: „Informacinės technologijos. XVI tarpuniversitetinė magistrantų ir doktorantų konferencija.“, 2011.



WI-FI SAUGOS PROTOKOLŲ ĮTAKA ENERGIJOS SUVARTOJIMUI DELNINIUOSE KOMPIUTERIUOSE

Inga Gudaitytė

Kauno technologijos universitetas, Kompiuterių katedra, Studentų g. 50, Kaunas, Lietuva, inga.gudaityte@stud.ktu.lt

Santrauka. *Bevielio tinklo infrastruktūra remiasi „Wi-Fi" technologija, leidžiančia naudotis patikimu ir greitaeigiu interneto ryšiu bevieliu būdu. „Wi-Fi" tinklas gali būti naudojamas delninukų (angl. PDA) prisijungimui prie kompiuterių tinklo aprūpinto prieigos tašku (angl. access point). Šis ryšys užtikrina saugią informacijos persiuntimo terpę, kai naudojamasi bevielio tinklo saugumo technologijomis WPA ar WPA2. WEP yra senesnis tinklo saugos metodas ir nėra saugus. Jungimasis per Wi-Fi sąsają įtakoja delninuko energijos suvartojimą. Šiame darbe dėmesys skiriamas delninuko baterijos energijos suvartojimui, priklausomai nuo pasirinkto saugos protokolo. Pateikiami energijos taupymo rėžimai mobiliems įrenginiams, aptariami saugos protokolai. Aprašomas energijos sunaudojimo įvertinimo metodas ir atliktų eksperimentų metodika. Remiantis gautais rezultatais, daromos išvados apie saugos protokolų pasirinkimą.*

Raktiniai žodžiai: saugos protokolai, energijos sunaudojimas, delninis kompiuteris, Wi-Fi technologija.

1 Įžanga

Visų elektroninių prietaisų naudojimas paremtas energijos vartojimu. Ne išimtis nešiojami kompiuteriai, mobilieji bei sumanieji telefonai, kurie naudoja pakraunamas baterijas. Baterijų veikimo laikas yra trumpas, todėl šie prietaisai linkę labai greitai išsikrauti. Kadangi šios technologijos yra populiarios, jose įdiegiama vis daugiau funkcijų, kurių naudojimas tik paspartina baterijos išsikrovimą.

Delniniai kompiuteriai yra naudojami komunikacijai su kitais kompiuteriais bei prieigai prie interneto resursų, todėl yra svarbu užtikrinti norimos persiųsti informacijos saugumą. Šiai funkcijai užtikrinti naudojami saugos protokolai. Bevielė tinklo infrastruktūra remiasi tokiomis kaip „Wi-Fi", „Bluetooth", „WiMax" technologijomis. Mūsų dėmesys skirtas Wi-Fi technologijai, nes jos palaikymas įdiegtas visose populiariausiose operacinėse sistemose, ji komplektuojama daugelyje šiuolaikinių nešiojamų bei delninių kompiuterių.

Darbo tikslas – sudaryti matavimo metodiką, kurios pagalba galima įvertinti energijos suvartojimą priklausomai nuo pasirinkto Wi-Fi saugos protokolo delninuke. Juos ištyrus bus galima patarti kokį saugos protokolą pasirinkti priklausomai nuo naudojamų funkcijų delniniame kompiuteryje, bei pasiūlyti sprendimą mažesniam energijos suvartojimui. Tyrimas įgyvendinamas su ASUS P750 delninuku, veikiančiu Windows Mobile aplinkoje.

2 Bevielių tinklų energijos taupymo sprendimai

2.1 Energijos taupymo rėžimai mobiliems įrenginiams

IEEE 802.11b specifikacija kontroliuoja duomenų persiuntimus tarp fizinio sluoksnio (radijo ryšio) ir jo apibrėžto prieigos prie terpės valdymo (angl. *MAC*) sluoksnio. Tinklas palaiko visas MAC sluoksnio funkcijas keisdamasis kontrolės kadrų serijomis, prieš tai leisdamas siųsti duomenis aukštesniems sluoksniams. Jis taip pat nustato kelis parametrus tinklo adapteriui. Vienas iš jų yra energijos rėžimas. Tinklo adapteris palaiko du rėžimus: aktyvų rėžimą (angl. *active mode*) ir energijos taupymo rėžimą (angl. *power save polling mode*). Pirmajame rėžime radijo imtuvas yra aktyvioje būsenoje ir visada vartoja energiją, tai leidžia jam priimti duomenis bet kuriuo laiku. Antrajame imtuvas dažniausiai būna laukimo būsenoje, tačiau periodiškai duoda užklausą prieigos taškui dėl naujų pranešimų. Todėl šis rėžimas sumažina baterijos energijos suvartojimą nešiojamuose ir delniniuose kompiuteriuose[1,2,4].

Dinaminis energijos valdymo metodas (DEV) (angl. *dynamic power management*) skirtas sutelkti dėmesį į bevielio tinklo kortos kontrolę, sumažinant energijos suvartojimą jos veikimo metu[7,8]. Apimamas metodų rinkinys, kuris siekia efektyvaus energijos vartojimo mažėjimo, išjungiant visus ar tik mažinant vykdomų sistemos komponentų skaičių, kai jie yra laukimo būsenoje. Energijos valdymo sistemoje komponentus galima nustatyti į skirtingas būsenas, kuriose kiekviena pasižymėtų skirtingomis savybėmis ir energijos naudojimo lygiu. Pavyzdžiui, sistemos komponentai gali turėti aktyvią būseną, laukimo būseną ir miego būseną, kuriose energijos vartojimas yra minimalus. Perėjimas tarp šių būsenų yra kontroliuojamas energijos valdymo modulio, kuris stebi sistemos apkrovą ir atsižvelgiant į anksčiau atliktus sistemos veiksmus, darbo krūvį ir veiklos apribojimus, nusprendžia, kuriuo laiku, kokia būsena bus pasirinkta.

Dažniausiai naudojamas DEV algoritmų rinkinys paremtas pertrūkių strategija. Jų trūkumas tas, kad jie nereikalingai naudoja energiją, laukdami, kol pereis į mažai energijos naudojančią būseną. Antras DEV algoritmų rinkinys remiasi elgesio prognozavimu sekančiam laiko periodui. Komponentas bus dedamas į mažos energijos rėžimą, jeigu jis nėra šiuo metu naudojamas ir valdymo modulis prognozuoja didesnį neveiklumo laiką. Trečias algoritmų rinkinys yra atsitiktinių algoritmų, kurie remiasi komponento prašymo aktyvuoti pasiskirstymu. Šie pasiskirstymai gaunami modeliuojant ar stebint įvykius sistemoje per tam tikrą laikotarpį[8].

3 Wi-Fi bevielio ryšio įrenginių naudojami saugos protokolai

Norint, kad Wi-Fi bevielis ryšys užtikrintų saugų informacijos persiuntimą, naudojami bevielio tinklo saugos protokolai. Pirmasis buvo sukurtas WEP protokolas, kuris stengėsi suderinti konfidencialumo, prieigos kontrolės ir duomenų vientisumą bevieliame tinkle[3]. Deja, protokole buvo rasta trūkumų. Po šių trūkumų aptikimo, buvo sukurtas WPA, kuriame išlaikytas tas pats kodavimo algoritmas RC4, tačiau įvestas naujas rakto valdymo mechanizmas TKIP (Temporal Key Integrity Protocol). Autentifikavimui buvo pridėti IEEE 802.1x ir iš anksto numatytų raktų (Pre-Shared Key) mechanizmai. PSK naudojamas bevielio ryšio sesijų metu identifikavimo raktams kurti.

WPA buvo tik laikinas sprendimas, todėl pagrindinės WEP problemos paskatino IEEE 802.11i standarto sukūrimą ir jo realizavimą kaip WPA2 protokolą. Jis naudoja skaitiklio rėžimą (Counter Mode) su CBC-MAC protokolu (CCMP) vietoj TKIP, taip pat reikalingas prietaisų tvirtinimas. Šifravimui (CTR mode) ir duomenų vientisumui (CBC-MAC) naudojamas AES algoritmas. Autentifikavimui naudoja du rėžimus: IEEE 802.1x ir PSK. Naudojant pirmąjį rėžimą, autentifikavimo metu yra kreipiamasi į autentifikavimo serverį pvz. RADIUS. O naudojant PSK metodą raktas rankiniu būdu įvedamas į kiekvieną bevielio tinklo prietaisą. WPA pagal PSK autentifikavimą yra skirtas mažų tarnybų, namų bevieliams tinklams ir neturi autentifikacijos serverių, bet vis tiek turi saugumo privalumų prieš WEP protokolą[3,6].

TKIP įgyvendina maišymo funkciją, kuri apima slaptą naudotojo raktą su inicializacijos vektoriumi, prieš pereidama į RC4 inicializaciją (RC4 srautinį šifravimą su 128 bitų raktu šifravimui ir 64 bitų raktu autentifikavimui). Taip pat TKIP įgyvendina 64 bitų žinutę, pavadintą MICHAEL, vientisumui patikrinti. Tačiau buvo įrodyta, kad TKIP šifravimo metodas gali būti nulaužtas[5].

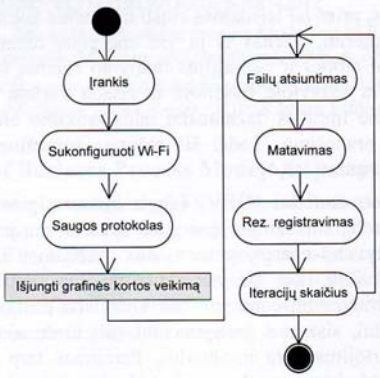
Mūsų atliktame tyrime bus ištirtas kiekvieno saugos protokolo sunaudojamas energijos kiekis, siunčiant duomenis tarp vartotojo ir serverio.

4 Energijos suvartojimo naudojant bevielę technologiją įvertinimo metodika

Naudojantis beviele Wi-Fi technologija, siunčiami failai iš serverio į delninį kompiuterį. Šis kelias gali būti neapsaugotas – be saugos protokolo, arba apsaugotas – WEP, WPA ar WPA2 protokolu. Pasirinkus atitinkamą saugumo būseną ištiriamas energijos suvartojimas siunčiant failus. Mūsų tyrime energijos suvartojimą delninuke lemia procesorius, atmintis ir Wi-Fi technologija.

Kuriamas įrankis imituos naudotojo veiksmus. Tyrimo pradžioje serveryje ir delniniame kompiuteryje sukonfigūruojami pasirinkti Wi-Fi saugos protokolo parametrai. Sukurtame įrankyje prieš pradedant matavimus išjungiamas grafinės kortos veikimas, norint gauti kuo tikslesnius matavimus. Paleidus vykdyti, atsiunčiami failai, atliekami matavimai, kurie registruojami rezultatų faile (1 pav.). Atlikus eksperimentą, be saugos protokolo ir su juo, gaunamas suvartotos energijos skirtumas (1).

Be saugos protokolo(BSP) – Su saugos protokolu(SSP) = energijos skirtumas. (1)



1 pav. Energijos suvartojimo įvertinimo metodas

Tyrimams atlikti pasirenkamas iteracijų skaičius, kuris nustatomas praktiniu būdu, pagal gautus duomenis panaudojus 100 iteracijų ir gavus rezultatus. Energija matuojama su pilnai įkrauta baterija (100-99%) iki kritinės talpos (30-20%). Pasiekus šią ribą, baterijos talpos matuoklis rodo netikslius duomenis. Bandymas atliekamas kelis kartus, tomis pačiomis sąlygomis.

5 Eksperimentas

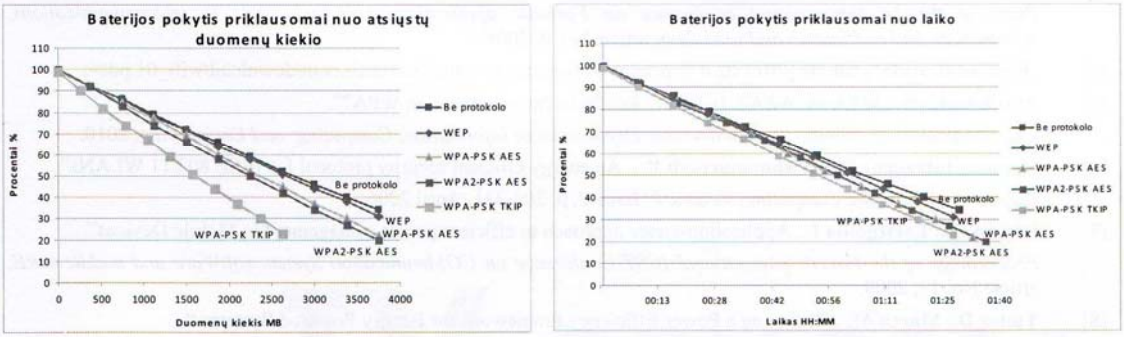
Tyrimui naudojamas prieigos taškas D-Link AirPlus DI-524, kurio parametrai: 802.11g standartas, perdavimo greitis iki 54Mbps, veikia 2,4GHz dažnių diapazone, ir delninis kompiuteris ASUS P750, kurio parametrai: Pocket PC platforma, PXA270 520 MHz procesorius, 64 RAM atmintis, Windows Mobile 6 Professional operacinė sistema, 1.3 baterijos versija.

Eksperimentas atliekamas su etaloniniu failu. Pasirinktas grafinio vaizdo failo formatas – bmp. Šio failo dydis – 786,486 baitai. Prieigos taškas ir delninis kompiuteris sukonfigūruojami prieš kiekvieną tyrimą (1 lentelė). Eksperimento metu delninio kompiuterio ekranas išjungiamas, kad tai neturėtų įtakos gaunamiems rezultatams. Rezultatai įrašomi į tekstinį failą, po to perkeliami į stacionarų kompiuterį ir apdorojami. Po kiekvieno tyrimo, akumuliatorius vėl pilnai įkraunamas.

Lentelė Nr.1 Delninuko ASUS P750 ir prieigos taško konfigūracijos parametrai

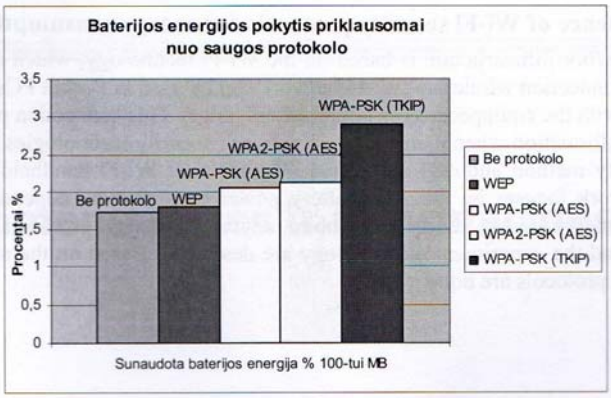
Saugos protokolas	Duomenų šifravimo algoritmas	Tinklo raktas
Be protokolo	–	–
WEP	128Bit	10 simbolių
WPA-PSK	AES	10 simbolių
WPA-PSK	TKIP	10 simbolių
WPA2-PSK	AES	10 simbolių

Iš gautų rezultatų brėžiame grafikus (2-3 pav.). Matome, kad siunčiant duomenis daugiausiai energijos sunaudoja WPA-PSK TKIP saugos protokolas. Atsiųstas duomenų kiekis žymiai mažesnis, nei naudojant kitus protokolus.



a) b)

2 pav. Delninuko baterijos pokytis, priklausomai nuo a) atsiųstų duomenų kiekio b) laiko.



3 pav. Baterijos sunaudota energija(%) 100 MB duomenų atsiuntimui.

6 Išvados

Rasti sprendimai, kurie naudojami energijos sąnaudų mažinimui. Šie sprendimai pagrįsti būsenų kontrole. Mūsų tyrimas vykdomas aktyvioje būsenoje, kai siunčiamas failas, todėl energijos suvartojimą įtakos pasirinktas saugos protokolas. Sprendimų, kuriuose būtų tirta mūsų problema, nebuvo rasta.

Aptarus saugos protokolus, galima teigti, jog WEP protokolas yra silpniausias, todėl pasirinkti jį nepatartina.WPA2-PSK(AES) stipresnis nei WPA-PSK(TKIP).

Sudaryta energijos sunaudojimo įvertinimo metodika, pagal kurią atliktas eksperimentas ir gauti rezultatai, nurodantys energijos suvartojimą pagal pasirinktą Wi-Fi saugos protokolą. Tyrimas patvirtino hipotezę, kad nenaudojant saugos protokolo, arba naudojant silpniausią WEP, energijos sąnaudos mažesnės, nei pasirinkus kitus protokolus (WPA –PSK, WPA2 –PSK).

WEP palyginus su WPA-PSK (TKIP), sunaudojama trečdaliu mažiau energijos, tačiau jų saugos lygis skiriasi. Rezultatai, naudojant WEP saugos protokolą, ir nenaudojant jokio, skyrėsi nežymiai (68%, 65%), todėl galime patarti siunčiant duomenis bevieliu tinklu tarp PDA ir kompiuterio naudoti bent WEP saugos protokolą. Norint stipriau apsaugoti duomenis, galima rinktis WPA-PSK(AES), WPA2-PSK(AES), WPA-PSK(TKIP), kurie šimto megabaitų duomenų atsiuntimui sunaudoja atitinkamai (2,05%, 2,13%, 2,9%,) energijos.

Turint tyrimo rezultatus, vartotojas gali pats pasirinkti saugos protokolą, įvertinant siunčiamos informacijos saugumo poreikį ir esamą delninio kompiuterio baterijos energijos likutį. Saugumo atžvilgiu[5] ir sunaudotos energijos kiekiu (3pav.), mes rekomenduotume pasirinkti WPA-PSK(AES) saugos protokolą.

Literatūros sąrašas

[1] **Adams J.** „Adaptive Buffer Power Save Mechanism for Mobile Multimedia Streaming".
Presented for the degree of Masters in Engineering to the School of Electronic Engineering Facullty of Vomputing and Engineergind Dublin City University Ireland, p.114, 2007.

[2] **Anastasi G., Conti M., Gregori E., Passarella A.** „802.11 power-saving mode for mobile computing in Wi-Fi hotspots: Limitations, enhancements and open issues".
Kluver Academic Publishers, *Wireless Networks,* Volume 14, Issue 6, p.745-768, 2008.

[3] **Bullbul H.I., Batmaz I., Ozel M.** „Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols".
Proc. of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, article No. 9, 2008.

[4] „How wi-fi works", žiūrėta [2011.02.07], prieiga per internetą: <http://nostarch.com/download/wifi_01.pdf>.

[5] **Frank H. Katz.** „WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?".
Source: Armstrong Atlantic State University. Department of Information, Computing, and Engineering, 2010.

[6] **Keeratiwintakorna P., Krishnamurthyb P.** „ An energy efficient security protocol for IEEE 802.11 WLANs".
Pervasive and Mobile Computing, Volume 2, Issue 2, p. 204-231, April 2006.

[7] **Lago A. B., Larizgoitia I.** „Application-aware approach to efficient power management in Mobile Devices".
Proceedings of the Fourth International ICST Conference on COMmunication System softWare and middlewaRE, article No: 11, 2009.

[8] **Tudor D., Marcu M.** „Designing a Power Efficiency Framework for Battery Powered Systems."
Source: ACM International Conference Proceeding Series, Proceedings of SYSTOR 2009: The Israeli Experimental Systems Conference, article No: 5, 2009.

Influence of Wi-Fi security protocols for energy consumption in PDA

Wireless network infrastructure is based on the Wi-Fi technology, which allows access to reliable and high-speed Internet connection wirelessly. Wi-Fi network can be used in Pocket PCs (called PDAs) to connect to a computer network with the equipped access point (access point). This connection provides a secure medium for the transmission of information when using wireless network security technologies, WPA or WPA2. WEP is an older network security method and it is not secure. Merger over Wi-Fi handheld interface influences energy consumption. This work focuses on the pda's battery power consumption, depending on the selected security protocol. Provided energy-saving mode for mobile devices, security protocols are discussed. The energy assessment method and the experiment methodology are described. Based on the results, the conclusions about the choice of security protocols are done.