LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

Sietveida topoloģijas tīklu iespēju pētīšana un analīze

BAKALAURA DARBS

Autors: **Oskars Zandersons**
Studenta apliecības Nr.: oz11012
Darba vadītājs: Dr.dat. Leo Trukšāns

RĪGA 2015

ANOTĀCIJA

Bakalaura darbs ir veltīts sietveida topoloģijas tīkliem. Bakalaura darbā tiks pētītas šādu tīklu pielietošanas iespējas, darbības īpatnības un īpašības.

Darba beigās tiks iegūts un apkopots liels daudzums kvalitatīvas informācijas par sietveida topoloģijas pielietojumu praktiskā līmenī mūdsienās, kā arī par perspektīviem pētījumiem globāla sietveita tīkla izveidē.

Darbā ir praktiski apskatīts un izmēģināts Hyperboria tīkls, kurš strādā uz, arī izpētīta darba ietvaros, cjdns protokola pamata.

Darbā iekļautas zināšanas par sietveida tīkliem, to īpašībām, izmantojumu un perspektīvām, par cjdns un citiem protokoliem ļoti lielu sietveida tīklu efektīvai maršrutēšanai, kā arī par Hyperboria tīklu. Darbs ir interesants gan tīmekļa lietotājiem, gan tīklu administratoriem, kuri varētu izmantot darbā esošas zināšanas par sietveida tīkliem.

Atslēgas vārdi: sietveida tīkli, sietveida topoloģija, Hyperboria, cjdns, Netsukuku, globāls sietveida tīkls, bezvadu sietveida tīkls, Guifi.

ABSTRACT

Bachelor thesis is devoted to mesh topology networks. In this Bachelor thesis will be explored mesh topology network possibilities and nature of activites and properties.

At the end of thesis there will be obtained and collated large amount of quality information about theme and practical level of mesh usage as well as for perspectives in future creating global mesh network.

At the thesis there is description of practical experiment and testing the Hyperboria network, which is working using cjdns protocol.

The thesis includes knowldge about mesh topology networks and perspective global mesh network boulding. Thesis is specially interesting for network users and also administrators, which could use it in their professional activities.

Keywords: mesh networks, mesh topology, Hyperboria, cjdns, Netsukuku, global mesh network, wireless mesh networks, Guifi.

SATURA RĀDĪTĀJS

APZĪMĒJUMI

IPv6 – Interneta Protokola versija 6 ir Interneta Protokola (IP) versija

IP – tīkla slāņa datu pārraides protokols, kuru lieto internetā.

Hyperboria – eksperimentāls tīkls, kurš radīts, lai izmēģināt cjdns protokolu darbībā.

Cjdns – tīkla protokols un tā realizācija, kas ļauj veidot mērrogojamu, drošu un vienkāršu konfigurēšanā tīklu.

DNS – Domain Name System, protokols, kas pārveido nosaukumus par skaitliskajām IP adresēm.

I2P – Invisible Internet Protocol, atvērtā koda programmatūra, kas ļauj organizēt īpaši bojājumpiecietīgu, anonīmu, overlay režēma, šifrētu, tīklu un ir pielietojama anonīmai Internet tīkla pārlūkošanai, hostingu veidošanau u.t.t. Adreses tīklā atrodas pseidodomēnu telpā .i2p.

Tor – Tor ir brīvprogrammatūra, kas nodrošina anonimitāti internetā un palīdz apiet cenzūru. Tā ir izstrādāta, lai lietotāji varētu izmantot internetu anonīmi tā, lai to darbības un atrašanās vietu nevar noskaidrot.

IEEE 802.11s – protokols, kurš ļauj organizēt hierarhiskus bezvadu ad hoc tīklus ar mobiliem un statiskiem mezgliem, sietveida tīklus, paplašina bezvadu piekļuves Internet tīklam funkcnionalitāti un ļauj realizēt bezvadu piekļuves punktus ar daudz plašāku diapazonu nekā standarta piekļuves punkti.

B.A.T.M.A.N. – maršrutēšanas protokols, kas tiek izstrādāst ar mērķi aizvietot OLSR protokolu.

OLSR – proaktīvs maršrutēšanas protokols, kas izmanto sasveicināšanās un kontrolēs ziņojumus, lai saņemt informāciju par tīkla topoloģiju.

Netsukuku – sadalīta, pašorganizējoša, vienranga, sietveida tīkla radīšanas projekts, kurš varētu pie minimāliem resursu tēriņiem nodrošināt maksimālu mezglu skaitu.

IRC – Tērzēšanas retranslēšana tīklā Internet (Internet Relay Chat) jeb IRC ir tūlītējās saziņas veids, izmantojot Internetu.

HTTP – hiperteksta transporta protokols (HyperText Transfer Protocol) ir lietojumslāņa protokols, kas paredzēts datu apmaiņai starptīmekļa serveriem un pārlūkprogrammām.

Telnet – Interneta protokols, kas pieder pie TCP/IP protokolu saimes un ko izmanto attālai piekļuvei tīkla resursiem un termināļu emulēšanai.

SQUID – programmatūras kopne, kas realizē kešējošā proxy servera funkciju protokoliem HTTP, FTP, Gopher un, atbilstošas konfigurācijas gadījumā, HTTPS.

DHCP – Dynamic Host Configuration Protocol, lietojuma slāņa protokols, kuru lieto, lai automātiski iedalītu IP adreses un citus uzstādījumus tīkla datoriem.

OSI – Open Systems Interconnection, konceptuāls komunikāciju sistēmas modelis.

MANET – Mobile Ad hoc Network, bezvadu, decentralizēti, pašorganizējošies tīkli, kas sastāv no mobilajām ierīcēm.

DD-WRT – ir Linux balstīta atvērtā koda programmatūra, piemērota ļoti dažādu veidu bezvadu maršrutētājiem un iegultajām sistēmām.

VPN – Virtual private network ir vispārējs nosaukums tehnoloģijām, kuras nodrošina vienu vai vairākus tīkla savienojumus (virtuālu tīklu) kāda tīkla vai vairāku tīklu (piemēram, interneta) ietvaros. Lai nodrošinātu datu nepārtveršanu publiskajos tīklos, tiek izmantota kriptogrāfija.

Guifi – vislielākais sietveida bezvadu tīkls pasaulē, kurš ir izveidots Katalonijā un Valensijā – Spānijā.

AWMN – Athens Wireles Metropolithan Network ir grieķu sietveida bezvadu tīkla projekts, kas aizsākās 2003. gadā.

QSPN – Quantum Shortest Path Netsukuku, jauns metaalgoritms, kurš, izmantojot fraktāļus, spēj izvietot liela tīkla karti failā, kas nav lielāks par diviem kilobaitiem.

MIMT – man-in-the-middle attack, ir uzbrukums tīklos, kas uzbrucējs slepeni pārtver komunikāciju starp diviem komunicējošiem un kuru trafiks iet caur pārtvērēja mezglu vai pārtvērējs ir pieslēdzies mazglam starp komunicējošiem.

IEVADS

Sietveida topoloģijas tīkli ir īpaši bojājumpiecietīgi salīdzinot ar jebkādas citas topoloģijas tīkliem, sniedz augstas decentralizācijas, privātuma un anonimitātes realizēšanas iespējas globālā mērogā, taču ir sarežģīti konfigurējami un prasīgi pret tīkla fizisko infrastruktūru [1]. Šāda veida tīklus var realizēt gan fiziskā veidā gan loģiski, izmantojot cita tīkla fizisko vidi. Darba problēma ir izzināt izmantošanas iespējas un perspektīvas, kā arī pašreizējo sietveida topoloģijas pielietojumu praksē, un atbildēt uz jautājumu – vai sietveida topoloģija varētu klūt par globāla tīkla pamata topoloģiju, kādas realizācijas tiek piedāvātas un kāda principā ir sietveida topoloģijas vieta mūsdienās un nākotnē.

Autors plāno pievērsties Hyperboria tīklam un cjdns protokolam, ar kuru tas strādā, kā risinājumam, kurš ir viens no tuvākajiem, strādājošajiem un attīstāmajiem mūsdienās, globāla sietveida tīkla implementēcijā.

Darba mērķis ir izpētīt un izanalizēt sietveida topoloģijas tīklu pielietošanu praksē kā arī pielietošanas perspektīvas, īpaši akcentējot uzmanību uz globāla sietveida topoloģijas tīkla izveides un darbības perspektīvām un jau esošiem realizācijas piedāvājumiem, apkopot iegūto informāciju un pētījumu rezultātus. Darbā paveiktais būs noderīgs sabiedrībai kā bagātīgs, apkopotas un papildinātas ar autora secinājumiem informācijas avots par perspektīvām sietveida topoloģijas tīklu izmantošanā un esošajiem protokoliem.

Darba rezultātā tiks iegūtas zināšanas par to, cik daudzveidīgs ir sietveida topoloģijas pielietojums tīklu veidošanā, kādi risinājumu eksistē pasaulē, kur tiek izmantota sietveida topoloģija tīkla veidošanā, tiks izpētīts, kur ir veidoti pilnvērtīgi sietveida bezvadu pašorganizējošies tīkli kā arī tiks izpētīti globāla mērroga risinājumi, kas sniedz svarīgas īpašības, kas raskturīgas sietveida topoloģijas tīkliem, kā arī tieši mēģinājumi izveidot globālu sietveida topoloģijas pašorganizējošos tīklu.

Par darba sverīgāko un interesantāko rezultātu autors uzskata Hyperboria tīkla un cjdns portokola izpētīšanu un izmēģināšanu un iegūstamās atziņas.

Mērķu un rezultātu sasniegšanai tiks izmantota dažādas literatūras pētīšana un analīze, tiks veikta salīdzināšana, kā arī tiks veikts praktiskt eksperiments, kura gaitā plānots uzstādīt un konfigurēt programmatūru, kā arī veidot tunelētu savienojumu ar tīklu Hyperboria caur Internet infrastruktūru.

Darbs sastāv no trim galvenajām nodaļā, kur pirmajā notiek iepazīšanās ar sietveida topoloģiju kā tādu, maršrutēšanas protokoliem, sietveida topoloģijas izmantojumu dažādiem mērķiem dažādos mēerogos. Otrajā nodaļā notiek teorētiska iepazīšanās ar globāla sietveida tīkla koncepciju, esošajiem risinājumiem globālā līmenī un ieskats Hyperboria tīkla un cjdns

protokolā kā šāda risinājuma pārstāvī. Trešajā nodaļā notiek detalizēta cjdns protkola un Hyperboria tīkla pētīšana teorētiskā līmenī un eksperimenta pieslēgšanās un konfigurēšanas veikšana praktiskā līmenī.

Darba beigās ir iegūto rezultātu nodaļa un nobeigums, kurā notiek secinājumu izdarīšana par paveikto darbu.

1. SIETVEIDA TOPOLOĢIJAS TĪKLI

Šajā nodaļā ir paredzēts apskatīt sietveida topoloģijas tīklus principā. Tiks apskatīti daži no svarīgākajiem protokoliem, uz kuru pamata ir iespējams vaidot šadus tīklus kā arī tiks apskatīti sietveida topoloģijas tīklu izmantojoms dažādām vajadzībām dažādos līmeņos – gan pilnvērtīga realizācija, gan daļēja realizācija, noteiktu īpašību iegūšanai. Īpaši interesanti darba ietvaros ir bezvadu pašorganizējošies sietveida tīkli.

1.1. Ievads

Lai zināt, kas ir sietveida topoloģijas tīkli, nepieciešams saprast, kas ir sietveida topoloģija. Sietveida topoloģija ir tāda tīkla topoloģija, kuras ietvaros katrs tīkla mezgls jeb iekārta ir savienota ar daudzām citām šī paša tīkla iekārtām vienā solī un visi mezgli var būt savstarpēji viena ranga nekontrolējama jeb pašorganizējoša tīkla gadījumā, vai arī dažādranga kontrolējama tīkla gadījumā [1,2,3]. Respektīvi sietveida topoloģijas tīkli ir tīkli, kas veidoti pēc šāda principa.

Sietveida topoloģijas tīkliem piemīt augstas decentralizācijas īpašības un ļoti augsta bojājumpiecietība [2]. Tā kā katra tīkla iekārta ir savienota ar jebkuru citu vairākos veidos, tad kāda no savienojumu bojājums neradīs traucējumus komunikācijā starp iekārtām.

Sietveida topoloģija ļauj apvienot tīklā lielu skaitu iekārtu un ir raksturīga parasti lieliem tīkliem [2]. Sietveida topoloģijas tīkli visbiežāk ir bezvadu.

Eksistē risinājumi, kas ļauj veidot un veido sietveida topoloģijas loģiskus tīklus pa virsu Internet infrastruktūrai ar mērķi paaugstināt privātumu, ieviest anonimitāti un šifrēt datus.

1.2. Protokoli un darbības principi

Mūsdienās sietveida topoloģijas tīkli tā vai citādi izplatās pa visu pasauli un veidojot šādus tīklus ir iespējams izvēlēties starp vairākiem protokoliem. Nozīmīgākos no tiem ir plānots apskatīt šajā apakšnodaļā. Tiks apakatīts protokols IEEE 802.11s, B.A.T.M.A.N., OLSR un salīdzinoši jaunais un augošais cjdns protokols.

1.2.1. IEEE 802.11s

IEEE 802.11s ļauj veidot kontrolējamus sietveida topoloģijas tīklus, teorētiski var izveidot arī nekontrolējamus(pašorganizējošos), bet šis standarts tam nav paredzēts [4].

Protokols nodarbojas ar maršrutēšanas tabulu atjaunināšanu tīkla ietvaros, tas darbojas OSI modeļa 2. līmenī [4], taču IP adreses ir nepieciešams piešķirt tradicionālā veidā – ar roku vai izmantojot DHCP [4].

Protokols atbild arī par kaimiņiekārtu atrašanu un mijiedarbību ar tām, kā arī par jaunu iekārtu integrāciju tīklā.

Tīkls var darboties kā ar paroli un būt noslēgts, tā arī bez tās, šifrēšana, kā parastā Wi-Fi tīklā, ir pieejama tikai līdz piekļuves punktam, ja tiek izmantota parole, nekāda tuneļveida end-to-end šifrēšana netiek realizēta [4].

Lai pieslēgties tīklam, kas veidots uz IEEE 802.11s pamata, nepieciešama iekārta, kas atbalsta šo standartu, nepieciešams zināt tīkla ID, kā arī segmentā nokonfigurēts un ieslēgts DHCP vai arī manuāli piešķirama adrese iekārtai. Un, protams, parole, ja tāda ir.

1.2.2. B.A.T.M.A.N.

B.A.T.M.A.N. ir maršrutēšanas protokols, radīts ar mērķi aizvietot OLSR [5]. B.A.T.M.A.N. var izmantot ne tikai MANET tīklu maršrutēšanā, bet arī citu bezvadu tīklu amršrutēšanā [5]. Galvenā B.A.T.M.A.N. īpašība un priekšrocība ir informācijas par labāko maršrutu decentralizācija – neviens mezgls tīklā nezin pilnus tīkla vai pat vienkārši labākā ceļa datus [5]. Izmantojot šo tehnoloģiju nav vairs nepieciešams sūtīt katram tīkla mezglam informāciju par izmaiņam tīklā. Katrs tīkla mezgls glabā tikai virzienu, no kura ienāk dati, kā arī nosūta tos. Tādā veidā mezgli nodot cits citam paketes, kuras ceļo pa dinamiski radītiem ceļiem [5].

B.A.T.M.A.N. piemīt arī klasiski maršrutēšanas prokololu elementi: tas var atrast citus B.A.T.M.A.N. tīkla mezglus un atrast labāko ceļu līdz tiem kā arī informēt kaimuņus par jaunu mezglu parādīšanos [5].

Katrs mezgls regulāri nosūta apraides signālus ar informāciju par savu eksistenci saviem kaimiņiem. Kaimiņi turpina nodot šo ziņu tālāk un tā tālāk. Tādā veidā katrs tīkla mezgls saņem šo informāciju [5].

B.A.T.M.A.N. nemēģina noteikt pilnu ceļu līdz paketes adresātam, bet nosaka tikai pirmo soli nepieciešamajā virzienā, un nosūta datus kaimiņam noteiktajā virzienā, kurš pielieto tādu pašu mehānismu. Process atkārtojas, līdz adresāts ir sasniegts [5].

B.A.T.M.A.N. var lietot ne tikai bezvadu tīklos, bet arī vadu vides datu pārraides tīklos, piemēram Ethernet [5].

1.2.3. OLSR

OLSR ir maršrutēšanas protokols MANET tīkliem, kurš, protams, ka var tikt izmantots arī citiem bezvadu tīkliem. OLSR ir proaktīvs maršrutēšanas protokols, kurš izmanto apmaiņu ar ziņojumiem, lai iegūt un kontrolēt informāciju par topoloģijas izmaiņām un stāvokli [6]. Tīkla mezgli izmanto šo informāciju, lai noteikt nākamo paketes lēcienu adresāta virzienā. OLSR ir viens no populārākajiem protokoliem, ko izmanto bezvadu MANET tīklu maršrutēšanā [6].

OLSR protokolā tīkla topoloģija atjaunināsˌ izmantojot apraides mehānismu [6]. Protokola īpatnība ir tāda, ka šī informācija ir zināma katram tīkla mezglam. OLSR mezgls nosūta sasveicināšanās ziņojumu. Izmaiņas topoloģijā tiek uzzinātas pateicoties no kaimiņiem saņemtajiem sasveicināšanās ziņojumiem. Šādos ziņojumos ir mezgla, kurš izsūtīja ziņojumu adrese, kā arī visu tam pieejamo kaimiņu saraksts. Tādā veidā mezgls paziņo saviem kaimiņiem par to, kādi savienojumi tam ir pieejami [6].

Katrs abonents glabā pie sevis informāciju par saviem kaimiņiem vienā solī un divos soļos. Sasveicināšanās ziņojumi tiek izsūtīti atkārtoti ar noteiktu intervālu, un, ja kādu laiku mezgls nepieņem sasveicināšanās ziņojumus no kaimiņa, tad savienojums ar viņu tiek uzskatīts par pārtrauktu. Atbilstošas izmaiņas tiek ieviestas topoloģijas tabulā.

Bez sasveicināšanās ziņojuma, periodiski tiek izsūtīts apraides topoloģijas kontroles ziņojums. Kontroles ziņojums satur informāciju par mezgla savienojumiem ar vienā solī savienotiem kaimiņiem. Izjot no informācijas, ko mezgls saņem no kontroles un sasveicināšanās ziņojumiem, tiek būvēts grafs, kurš apraksta īsākos ceļus informācijas nodošanai katram mezglam [6].

Šādā sakaru organizēšanā starp mezgliem ir viens liels trūkums. Ir dabiska situācija, kad divu soļu kaimiņš var būt viena soļa kaimiņš diviem vai vairākiem viena soļa kaimiņiem. Tādā gadījumā rodas situācija, kurā divu soļu kaimiņš saņems vienu un to pašu sasveicināšanās ziņojumu vairākas reizes. Lai šo situāciju atrisināt OLSR protokolā ir paredzēta ziņojumu izsūtīšanas optimizācijas metode MPR [6]. Pēc topoloģijas tabulas, mezgls izvēlas tādus viena soļa kaimiņus ar simetrisku savienojumu, kuri ir viena soļa kaimiņi vismaz vienam divu soļu kaimiņam dotajam mezglam.Šī metode ļauj samazināt apraides datu plūsmas.

1.2.4. CJDNS

Cjdns ir tīkla protokols un tā realizācija, ar kuru palīdzību ir iespējams radīt drošu, vienkārši konfigurējamu un mērrogojamu tīklu. Ar cjdns izveidots tīkls var strādāt gan izmantojot Internet infrastruktūru vai tunelējoties pa virsu Internet infrastruktūrai, gan arī izveidot tīklu izmantojot reālas fiziskas iekārtas, kas konfigurētas strādāt ar cjdns protokolu [7].

Protokola darbību nodrošina izmantojot tīkla tuneli. Programmas var strādāt dotajā tīklā pie nosacījuma, ka tās atbalsta protokolu IPv6. Pēc nepieciešamās programmatūras uzstādīšanas visas atbilstošās tīkla plūsmas novirzās un doto tīklu. Tīklā lietotāji saņem IPv6 adreses, kuras atbilst privātajam adrešu segmentam, tādējādi nenotiks kolīzijas starp īsto IPv6 Internet tīklu un cjdns tīklu. Pieslēdzotīes tīklam caur Internet tīklu ir nepieciešams atrast jau eksistējošu mezglu cjdns tīklā un uzzināt tā adresi un atslēgu. Pieslēdzoties fiziskam tīklam, viss notiek automātiski [7].

Datu plūsmu maršrutēšana notiek izmantotjot sistēmu, kas darbojas analoģiski Kademlia DHT [7] – maršrutu katalogs tiek patstāvīgi atjaunināts, ja tīkla konfigurācija mainās, tādā veidā tīkls uztur optimālu noslodzi tīkla mezgliem un izvēlas izdevīgāko un īsāko ceļu datu paketēm.

Cjdns protokols joprojām tiek attīstīts un ir diezgan jauns, taču pasaulē ir daudzas vietas, kur ir implementēti cjdns tīkli noteiktās ģeogrāfiskās vietās, kā arī strādā pazīstamais Hyperboria tīkls, kurš strādā pa virsu Internet tīklam un kuram var pieslēgt jebkuru fizisku tīklu, vai var pieslēgties no jebkuras vietas pasaulē arī pa virsu Internet tīklam.

Attēlā 1.1 ir redzama Austrumeiropas karte, kurā dažādi aktīvisti ir atzīmējušies kā cilvēki, kas uzstādījuši pie sevis ar cjdns protokolu strādājošu bezvadu iekārtu un ir gatavi savienoties tīklā. Kartē nav redzami visi šādi bezvadu cjdns punkti, jo vietne, kurā notiek pieteikšanās nav centralizēta oficiālā veidā un, iespējams ir arī citas sabiedrības, kas veido paralēli bezvadu tīklu, svarīgi, lai beigās visi savienojas kopā.

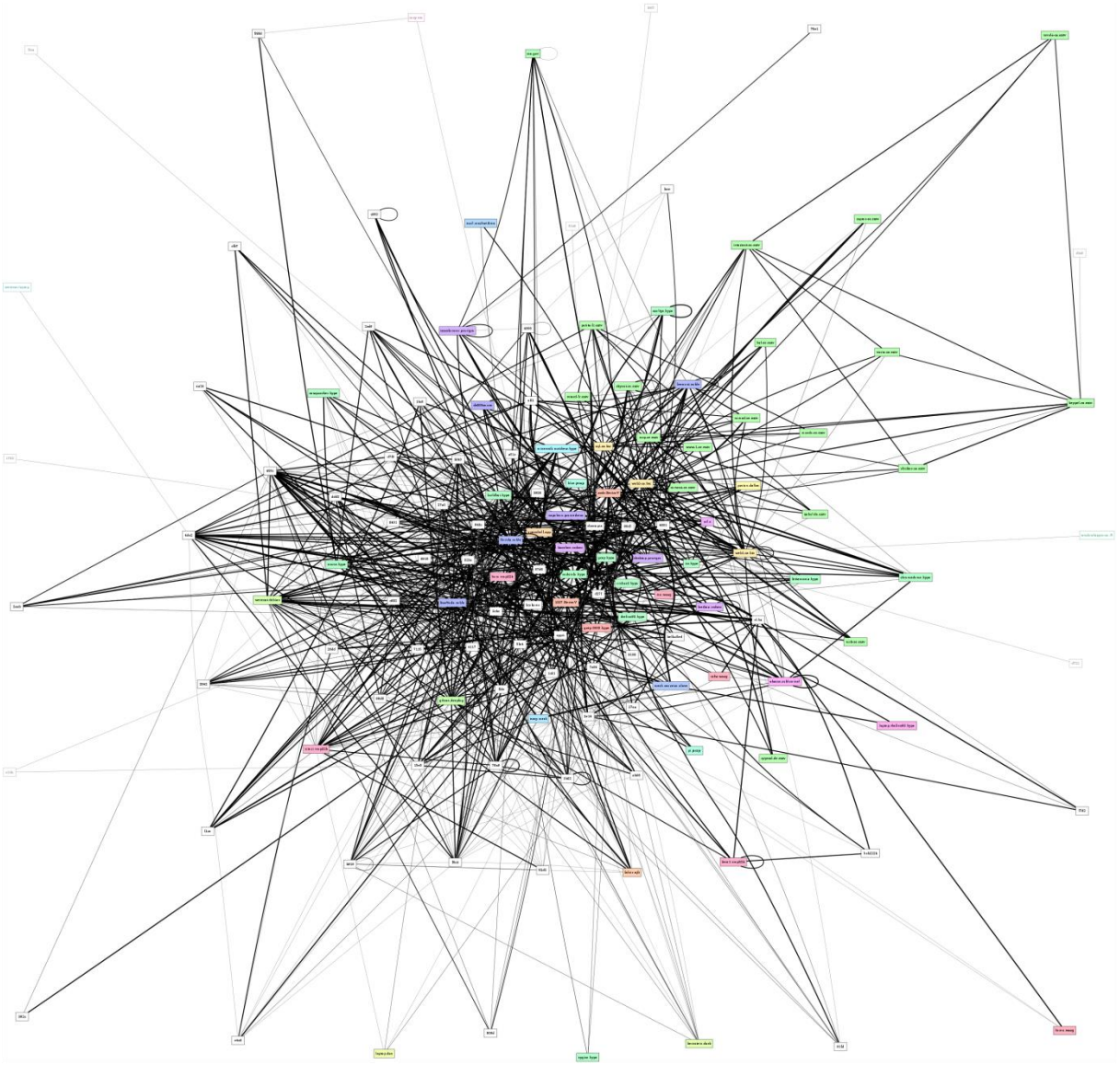
1.1. att. ***Austrumeiropas karte ar cjdns atbalstošām bezvadu iekārtām***

Jāpiebilst, ka visi attēlā redzamie punkti nav savienoti savā starpā un neveido vienotu tīklu, bet kalpo kā motivācija pievienoties jauniem lietotājiem līdz vienubrīd būs iespējams tehniski izveidot savienojumus, jo lietotāji būs gana tuvu viens otram, un apvienoties vienā tīklā. Kā redzams vesali trīs punkti ir arī Latvijas teritorijā. Divi Rīgā un viens netālu no Jēkabpils. Kā arī jāpiebilst, ka pieslēdzoties Hyperboria tīklam, lielākā daļa šo mezglu arī nav tajā, jo katrē ir atzīmēri apmēram 1500 mezglu, bet Hyperboria tīkls sastāv no ne vairāk kā 500, līdz ar to var izdarīt secinajumu, ka lielākā daļa šo punktu vēlas veidot tikai fizisku, pilnvērtīgu cjdns tīklu un vēl tikai gaida savu kārtu piedalīties lielā tīkla veidošanā.

Hyperboria tīkls nodrošina augstu privātuma līmeni un, ja tas tiktu realizēts tikai fiziskā veidā, izamatojot reālus bezvadu maršrutētājus, tad tas nodrošinātu arī anonimitāti. Bet tas darbojas arī Internet tīklā un tā mērķis nav anonimitāte un nav mērķis bijis kļūt par I2P/Tor klonu. Tādā veidā izmantojot trasēšanu ir iespējams iegūt mezglu virknīti un uzzināt lietotāja īsto IPv4 adresi. Tīkla datu plūsmas tiek šifrētas un nosūtītos datus spēj atšifrēt tikai adresāta mezgls.

Hyperboria tīkls tika radīts kā tīkls cjdns protokola testēšanai [7]. Tam var pieslēgties jebkurš, kurš vēlas, uzstādot atbilstošu programmatūru uz sava datora vai iekārtas. Šāds mēģinājums darba ietvaros tiek veikts un detalizēti aprakstīts atbilstošajā nodaļā.

Attēlā 1.2. ir redzama Hyperboria tīkla karte. Kā redzams attēlā, tad tīkls ir neliels, bet tajā ir ļoti daudz savienojumu. Tas arī ir sietveida princips, kur katram mezglam ir vairāki citi tāda paša ranga mezgli pievienoti un tas protams gan uzlabo veiktspēju, gan palielina bojājumpiecietību.



1.2. att. ***Hyperboria tīkla karte***

Hyperboria tika radīts kā tīkls, kurš ļaus nodot caur Internet tīklu datus droši nošifrētā veidā, bet tīkla lietošanas ātrums tiektos uz maksimāli iespējamo. Lai realizēt neatkarīgu decentralizētu DNS ir izstrādāts modulis uz krosplatformās pseidonīmu sistēmas Nxt bāzes [7,8].

1.3. Izmantojums un izmantojuma perspektīvas

Šajā nodaļā notiek iepazīšanās un aprakts tam, kādas ir jau praktiskas un realizētas, kā arī vēl perspektīvas iespējas pielietot sietveida topoloģijas tīklus ar mērķi sasniegt pilnu to realizāciju un izmantot iespējamās priekšrocības, vai arī izmantot sietveida topoloģijas īpašības kādā līmenī vai daļēji. Darba ietvaros īpaši interesanti ir jau radītie bezvadu sietveida tīkli dažādās vietās pasaulē.

1.3.1. Lokālos mērrogos

Šajā apakšnodaļā tiek apskatīti lokālie sietveida bezvadu tīkli, kas realizēti dažādās vietās pasaulē ar mērķiem, kā ērti, lēti un efektīvi izplatīt tīmekļa savienojumu vietās, kur klasiskā veidā pakalpojumu sniedzēji dažādu iesmeslu dēļ to nav izdarījuši vai nav izdarījušoi gana labi, gan arī tādi, kas tiek realizēti īpašān krīzes situācijās vai arī gluži vienkārši praktiskām sabiedriskām vajadzībām vai arī lokālo dienestu darbības uzlabošanai.

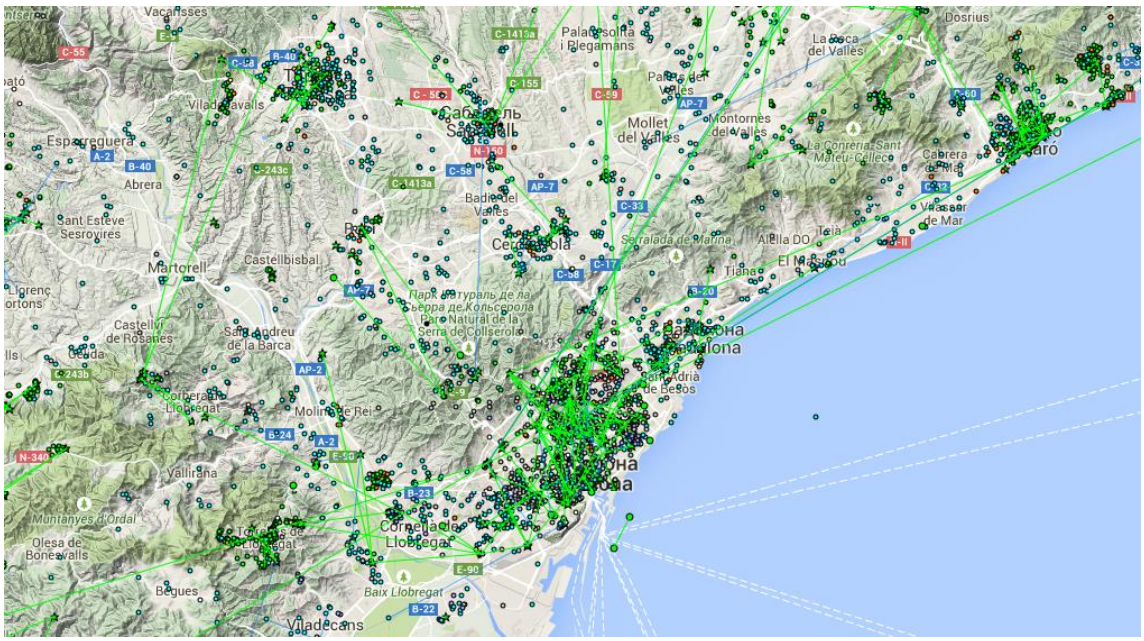
1.3.1.1. Guifi

Vislielākais sietveida bezvadu tīkls pasaulē ir izveidots Katalonijā un Valensijā [9]. Tie ir Spānijas reģioni. Tīkls sastāv no divdesmit dieviem tūkstošiem mezglu. Projekts radās XXI gs. pašā sākumā, kad vietējiem iedzīvotājiem apnika gaidīt līdz reģionā parādīsies apmierinošs vajadzības interneta pakalpojumu sniedzējs [9]. No tā laika pēc iedzīvotāju iniciatīvas un patstāvīgas praktiskās piedalīšanās attīstās Guifi un ir pieejams bez maksas.

Runājot vienkārši shēma ir sekojoša – ir nosacītas vienības – „saliņas". Katra saliņa ir viens pilnvērtīgs sietveida tīkls, kas apvieno rajona, pilsētas vai pašvaldības iedzīvotājus. Lai pieslēgties tīklam tiek izmantoti bezvadu maršrutētāji, kas korekti nokonfigurēti un par bāzes sistēmu izmanto DD-WRT. Sakari starp saliņām tiek nodrošināti izmantojot VPN serverus vai Squis proxy serverus. Šie paši serveri sniedz Guifi lietotājiem piekļuvi Internetam. Respektīvi, ja serveris kļūst nepieejams, saliņas turpina pilnvērtīgi strādāt, bet piekļuve citām saliņām vai Internetam pazūd [9].

Konkrēts savienojuma joslas platums un savienojuma stabilitāte ir dažāda, atkarībā no vietas, dažviet savienojuma joslas platums nepārsniedz 1 Mbit/s [9], taču daudzās vietās Guifi joprojām ir labākais iespējamais pieslēguma veids Internetam [9].

Attēlā 1.3. ir redzama Guifi tīkla karte. Centrālā pilsēta – Barselona. Guifi tīkls ir izaudzis dizgan plašos apjomos.



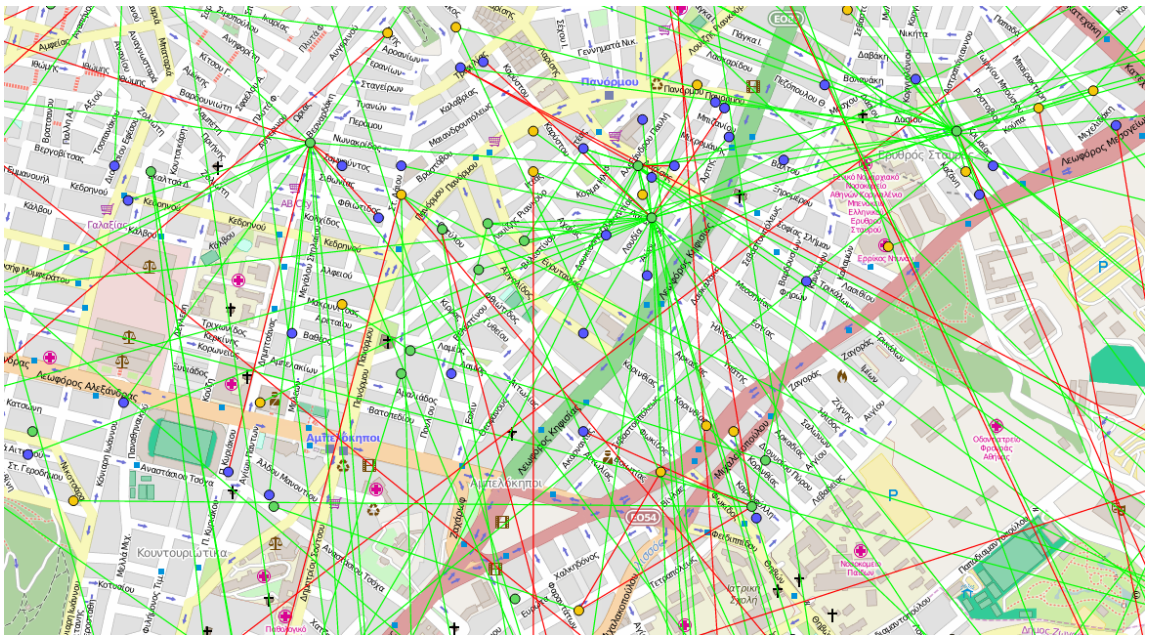
1.3. att. ***Guifi tīkla karte***

Kā redzams attēlā 1.3., tad attālinājums ir diezgan liels un var novērtēt apmērus, kādos ir attīstījies tīkls Guifi Spānijā, kā arī ir manāma sietveida topoloģijas, kas ir raksturīga šim tīklam.

1.3.1.2. AWMN

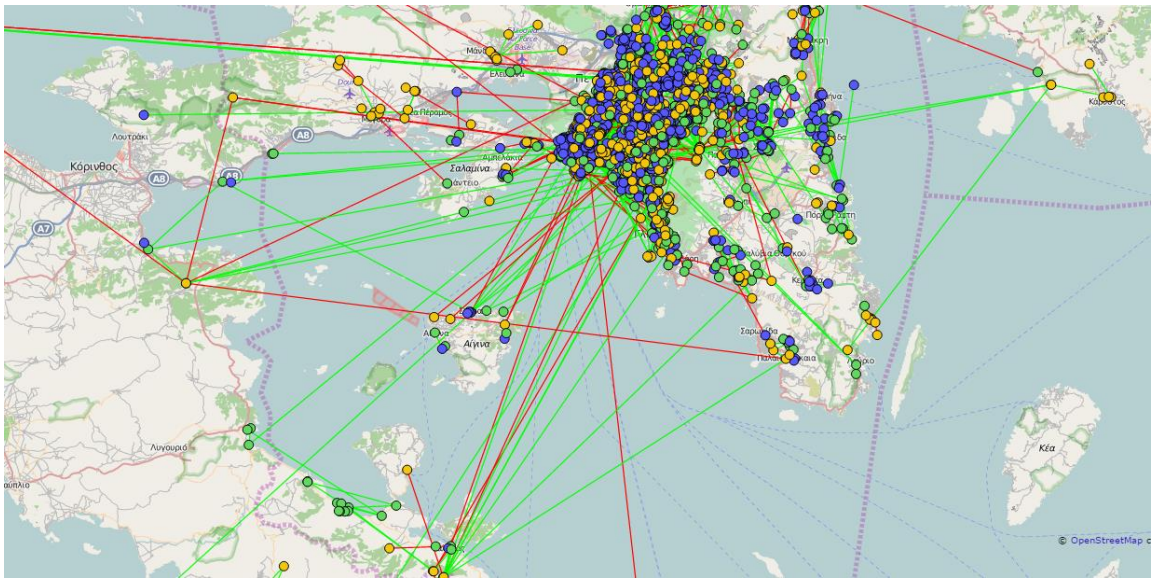
Athens Wireles Metropolithan Network ir grieķu sietveida bezvadu tīkla projekts, kas aizsākās 2003 [9]. gadā. Līdzīgi kā ar Guifi, atēniešu mērķis bija nodrošināt ātrpieslēguma internetu. Līdz brīdim, kas platjoslas pieslēguma pakalpojumi kļuva plaši pieejami Atēnās, AWMN jau izauga un nonāca līdz daudziem attālinātiem Grieķijas reģioniem un pat savienojās ar vienu mezglu Slovēnijā [9]. Kopumā projektā bija vairāk par tūkstoti virsmezglu, kuri apvienoja apmēram trīs tūkstoš lietotāju izmantojot maršrutēšanas protokolus BGP un OSLR [9].

Attēlā 1.4. ir redzams Atēnu bezvadu metropolijas tīkla fragments stiprā pietuvinajumā. Līdzīgi kā Gufi, ārī šis tīkls ir sabiedrības radīts un izplatīts.



1.4. att. ***AWMN tīkla karte tuvinājumā pilsētas mērogā***

Zamāk esošajā attēlā 1.5. autors vēlas parādīt, cik izplatīts ir kļuvis AWMN tīkls Grieķijas valsts mērogos, un ka ir pat izgājis ārpus tās robežām.



1.5. att. ***AWMN tīkla karte attālinājumā Gieķijas valsts mērogā***

Ņemot vērā šādu sietveida bezvadu lokāla tīkla strauju izaugsmi un izplatību vienas valsts mērogos, autors uzskata par iespējamu un ļoti interesantu šāda tīkla perspektīvu izplatīties globālos mērogos, kas arī ir lielā mērā dotā bakalaura darba interese.

Šāda veida tīkls sniegtu ne tikai lētu un vienkāršu tīmekļa izplatīšanu līdz katrai mājai ar automātiski atrisinātu pēdējās jūdzes problēmu, bet arī sniegtu lieliskus un praktiski neuzlaužamus privātuma aizsardzības mehānismus.

1.3.1.3 Komunikācijas modelēšana ārkārtas situācijās

Tā kā bezvadu sietveida topoloģijas tīkli nodrošina drošu un aizsargātu segumu noteiktā lokālā apgabalā, tad šī tehnoloģija tiek uzskatīta par efektīvu veidu kā nodrošināt mobilus, augsa ātruma savienojumus krīzes situācijās [2].

Šāds tīkls ir ļoti bojājumpiecietīgs un spēj pašatjaunoties un veiksmīgi turpināt darbu, ja notiek kādu mezglu izeja no ierindas. Tādas tīkla īpašības ļauj to ļoti ātri ieviest un izplatīt kā arī atjaunināt sabrukuma vai daļēja sabrukuma gadījumā. Šāds tīkls var tikt izveidots no nulles dažu stundu laikā, sliktākajā gadījumā dienas laikā kopš krīzes situācijas vai dabas katastrofas uzsākšanās.

Bieži vien, pilsētās un lielpilsētās arkārtas situāciju dienesti izmanto savas privātās, slēgtās komunikācijas sistēmas, kas strādā dažādās frekvencēs un katastrofas gadījumā dažādu dienestu darbinieki nevar efektīvi un ātri sazināties savā starpā [2]. Savukārt ja pilsētas teritorijā funkcionē bezvadu sietveida tīkls, tad visu ārkārtas dienestu darbinieki var pieslēgties kopējam tīklam, drošības nolūkos izmantojot paroli un pilnīgi drošā un šifrētā veidā sazināties savā starpā. Izmantojot šādu tīklu dati, kas tiek parraidīti tunelējas un ir norobežoti no tiem datiem, ko sūta lietotāji un kas neatiecas uz dienestu darbu [2]. Tas novērš nesankcionētu piekļuvi datiem.

1.3.2. Biznesa vajadzībām

Pirmkārt sietveida tīkli var tikt izmantoti biznesā. Piemēram, pilsētas ielās ir izvietoti daudzi apmaksas termināļi un bankas termināļi un viņi visi pieslēdzas Internetam, pamatā izmantojot 3G un 4G modemus, ko sniedz mobilo operatori [10]. No vienas puses, protams, ir labi, jo tas ir vienkāršs un labs risinājums, bet no citas puses, tas var izmaksāt dārgi un var gadīties lēns datu nodošanas ātrums [10].

Izmantojot sietveida bezvadu tīklu, ja pilsētas rajons jau ir noklāts ar šādu tīklu, tad papildus mezgls būs automātiski pieslēgts Internetam un pašam, piemēram, cjdns, ja ir izvēlēts šads variants, tīklam un respektīvi pats strādās kā retranslators un uzlabos kopējo signālu [10].

Bez tā, cjdns tīklā ir iespējama joslas rezervēšana [10] – situācijās, kad tīkls ir ļoti noslogots, datu plūsmas virziens var tiks izmainīts un tādējādi noslodze var tiks sadalīta, kas nodrošinās to, ka sakari nepazudīs piemēram kādu lielu svētku laikā, kā mēdz būt ar mobilajiem tīkliem Jaungada laikā.

1.3.3. Valsts vajadzībām

Var likties, kam gan kādai valstij sietveida pašorganizējošies tīkli, kas ir pēc savas dabas praktiski nekontrolējami. Iemesls ir vienkāršs – tas ir lētākais veids, kā nodrošināt piekļuvi Internetam [10]. Pēc būtības, ja tiek izvietots kādā mājā cjdns piekļuves punkts un pēc tam pēc sociālās programmas izdalīt konfigurētu maršrutētāju katram dzīvoklim, tas ievērojami atvielgo tīkla montāžu un palielina datu pārraides summāro ātrumu.

1.3.4. Pakalpojumu sniedzēju vajadzībām

Pakalpojumu sniedzēji var izmantot tās priekšrocības kas ir saistītas ar tīkla ieviešanas vienkāršību un lētumu. Protams, notiks nenovēršama demonopolizācija, kas ne visiem ir izdevīgi, taču ja būs vienots, piemēram, cjdns balstīts vai arī uz kāda līdzīga protokola balstīts bezvadu sietveida tīkls, tad tiks pilnībā atrisināta pēdējās jūdzes problēma [10]. Pakalpojumu sniedzēji varētu nodrošināt savienojumus starp tīkla segmentiem, un pārdot piekļuvi piekļuves punktiem, taču tas drīzumā varētu izzust, jo visticamāk rastot bezmaksas analogi, jo ieviests, piemēram cjdns tīkls būtu pašorganizēsošs un principā katrs ir pats sev pakalpojumu sniedzējs.

2. GLOBĀLS SIETVEIDA TĪKLS

Runājot par globālu sietveida tīklu, protams, ka tiek pamatā domāts bezvadu globāls sietveida tīkls, jo izveidot globālu vadu sietveida tīklu ir neefektīvi, neprātīgi un bezjēdzīgi, jo tiek zaudētas daudzas nozīmīgas īpašības, kas piemīt bezvadu tīklam un tas ir ļoti dārgi no materiālā viedokļa.

Šajā nodaļā paredzēts apskatīt, kāds tad īsti būtu ideāls globāls sietveida tīkls, kā arī apskatīt jau esošos risinājumus šāda tīkla izveides virzienā vai atsevišķu tā īpašību implementēšanas virzienā, jo realizēts šads tīkls pilnībā, kā manāms, vēl nav un tuvākajos gados visticamāk nebūs.

2.1. Privātums un anonimitāte

Runājot pat privātumu un anonimitāti, ir svarīgi nejaukt šos jēdzienus. Privātums ir aizsardzība pret nesankcionētu piekļūšanu, piemēram datiem, bet anonimitāte ir identitātes noslēpšana.

Tīklu kontekstā, par privātumu var tikt uzskatīta iespēja droši un šifrēti nosūtīt savus datus tikai adresātam, bez kādām nesanksionētām pārtveršanas un nolasīšanas iespējām, bet par anonimitāti var uzskatīt iespēju izmantot tīklu un tīkla pakalpojumus, nosūtīt datus, vai saņemt tos, bez iespējas izsekot un noteikt, kurš mezgls veica darbību.

Lai panākt anonimitāti Internet tīklā, tiek radīti virtuāli tīkli, kas strādā pa virsu Internet tīklam [11]. Šādi tīkli tiek radīti, meklējot kompromisu starp aizsardzības līmeni un tīkla veiktspēju. Parasti – lai panākt anonimitāti tiek zaudēta ātrdarbība, kā arī tiek iespējoti daudz lielāki datu plūsmu apjomi nekā nepieciešams vienkāršai datu pārraidei [11]. Šādos tīklos realizētā daudzlīmeņu šifrēšana un datu plūsmu sadalīšana vairākos ceļos padara par gandrīz nekaitīgu datu pārtveršanu vai pat kāda mezgla uzlaušanu un nesankcionētu piekļūšanu tam vai izvešanu no ierindas [11].

Šādi tīkli var tikt veidoti, lai nodrošināt anonimitāti vai privātumu, vai abus. Bakalaura darba kontekstā dziļāk apskatītais Hyperboria tīkls potenciāli var nodrošināt abus, ja tiktu realizēts bezvadu sietveida tīkla formā ar savienojumiem stapr maršrutētājiem fiziskā veidā, taču pašreizējajā formā, kad darbojas galvenokārt virtuāli pa virsu Internet tīklam, garantēti nodrošina tikai privātumu, jo izsekot mezgliem, izmantojot IPv4 reālās adreses ir iespējams.

Papildus var minēt speciāli izveidotos TOR un I2P tīklus, kā arī citus, kas darbojas overlay režīmā, jeb pa virsu Internet tīklam un nodrošina datu privātumu un anonimitāti ar savām metodēm. Tas tiks apskatīts nedaudz vēlāk šajā nodaļā.

2.2. Decentralizācija

Decentralizācija tīkla kontekstā nozīmē to, ka tīklā piedalās kāds daudzums tīkla iekārtu jeb tīkla mazglu, no kurām jebkura var sazināties ar jebkuru citu tiešā veidā. Jebkura iekārta var sūtīt pieprasījumus citām iekārtām sniegt piekļuvi kādiem tīkla resursiem un tādējādi būt klienta lomā. Esot servera lomā, katra iekārta ir spējīga apstrādāt pieprasījumus no citām iekārtām tīklā un atbildēt atbilstošā veidā uz pieprasījumiem [12].

Katra iekārta izpilda arī noteiktas administratīvas funkcijas, piemēram, glabāt savu kaimiņu iekārtu sarakstu un uzturēt šī saraksta aktualitāti [12].

Jebkurš tīkla loceklis negarantē savu pastāvīgu atrašanos tīklā, jebkura iekārta var jebkurā brīdī pazust vai parādīties tīklā. Kādā noteiktā tīkla kritiska izmēra sasniegšanas brīdī, tīklā eskistē daudzi serveri ar vienādām funkcijām [12].

Decentralizācija nozīmē to, ka tīklā nav kādi noteikti mezgli, no kuriem ir vitāli atkarīga visa tīkla darbība. Decentralizētā tīklā katrs mezgls ir pievienots vairākiem citiem, un dažu mezglu atteikums nav iemesls zaudēt piekļuvi tīklam citiem mezgliem.

Bakalaura darba kontekstā dziļāk apskatītais Hyperboria tīkls ir lielisks decentralizēta tīkla piemērs.

2.3. Pašorganizēšanās

Pašorganizējošos tīklu būtība ir ļaut tīkla lietotājam pieslēgties tīklam un lietot tā pakalpojumus nevis kādos konkrētos piekļuves punktos, bet pieslēdzoties caur citiem lietotājiem un tīkla mezgliem. Pašorganizējošies tīkli pilnīgi noteikti ir decentralizēti tīkli ar mainīgu tīkla struktūru [13].

Kopumā šādiem tīkliem piemīt vairākas nopietnas priekšrocības – tas ir plašs pārklājums un liels lietotāju skaits bez noteiktām, daudzām un dārgām piekļuves un izplatīšanas stacijām [13]. Runājot vienkārši – pašorganizējošs tīkls sastāv no liela skaita lietotāju, kur visi ir vienranga un ir savienoti cits ar citu, pie tam katrs – ar vairākiem citiem. Protams, ka šāds tīkls ir pamatā bezvadu, jo ir grūti pat iztēloties lietotājus, kas velk cits pie cita garu kabeli un kuru iekārtās ir lērums ar tīkla portiem.

Šādā tīklā katrs lietotājs principā palielina tīkla darbības rādiusu. Šī bakalaura darba kontekstā dziļāk pētītais Hyperboria tīkls ir pilnībā pašorganizējošs tīkls un kalpo par lielisku piemēru šāda vaida tīklam. Pašorganizācija lieliski demonstrēta tīkla testēšanas laikā, kad autoram izdodas pieslēgties paša spēkiem esošiem mezgliem tīklā un kļūt par vēl vienu mezglu, kuram kāds var pieslēgties.

Pašorganizējošos tīklos katras atsevišķas iekārtas jauda var nebūt liela, bet kopumā tīkls var izaugt ļoti liels ar augstu veiktspēju. Tas nozīmē, ka šādi tīkli ir lēts un efektīvs veids, ka savienot lietotājus tīklā. Pie tam, tā kā iekārtas ir nelielas jaudas, tad ir mazāk problēmu ar magnētiskajiem laukiem un to konfliktiem [13].

2.4. Daži esošie risinājumi un to īpatnības

Starp esošajām iespējām un risinājumiem globāla bezvadu pašorganizējošos sietveidu tīklu vaidošanā protams nav neviena pilnvērtīga globāla pašorganizējoša sietveida tīkla. Ja tāds būtu, to noteikti pamanītu visa sabiedrība, jo bez tās piedalīšanās šadu tīklu izveidot praktiski nav iespējams.

Esošie risinājumi lielākajā daļā gadījumu ir domāti, lai daļēji izpildīt dažas noteiktas globāla bezvadu sietveida tīkla īpašības, kas ir lietotājiem svarīgas un ir tehniski realizējamas mūsdienu realitātes apstākļos.

Kā viens no risinājumiem tiks apskatīts TOR tīkls un I2P tīkls. Šie abi ir tīkli, kas sniedz iespējas lietot tīkla pakalpojumus anonīmi un privāti. Abi tīkli strādā pa virsu Internet tīklam un izmantot tā resursus informācijas nodošanai. Šie tīkli nepretendē uz būšanu par bezvadu sietveida tīkliem, taču realizē dažas īpašības, kas ir būtiskas īpašības arī bezvadu sietveida tīklos, un realizē jau šodien un globāli, un pilnvērtīgi.

Tiks apskatīts arī Netsukuku tīkls, kas diemžēl neturpina attīstību, bet tika iecerēts savulaik kā tehnoloģijas pilnvērtīga bezvadu sietveida tīkla uzbūvēšanai un pēc paredzētā pielietojuma un īpašībām ir praktiski identisks jaunākajai un attīstāmajai Hyperboria platformai. Netsukuku ir bojājumpiecietīgs, decentralizēts, pašorganizējoš, bezvadu sietveida tīkls, kaz būvēts uz jau esošām tīkla tehnoloģijām, bet ne pa virsu Internet tīklam, bet kā patstāvīgs tīkls.

Un protams tiks apskatīts Hyperboria tīkls, kas strādā izmantojot cjdns protokolu un tā realizāciju.

2.4.1. I2P

I2P ir atvērtā koda programatūra, kas domāta, lai organizēt īpaši bojājumpiecietīgu, anonīmu, overlay režīma, šifrētu, privātu tīklu, kas būtu piemērots tīmekļa pārlūkošanai, anonīmam hostingam tīmeklī, sazināšanās sistēmām un failu apmaiņai, kā arī elektroniskajam pastam, VoIP servisiem in dažādām citām lietām [14,15]. Adreses I2P tīklā atrodas pseido domēnu vārdu telpā .i2p [14].

I2P ir interesanta darba kontekstā ar šifrēšanas mehānismu izmantošanu, vienranga arhitektūru un mainīgiem plūsmu starpniekiem. Šis viss palielina deanonimizācijas sarežģītību, nodrošina privātumu un novērš MIMT uzbrukumus, padara neiespējamu pakešu aizvietošanu lietotājam nemanot [14,15].

Tā kā tīkls ir vienranga un decentralizēts, tad tīkla darbības ātrums un uzticamība ir tieši atkarīga no lietotāju skaita un to piedalīšanās svešu datu plūsmu nodošanā caur savu infrastruktūru [14].

Lai piekļūs I2P tīklam, nepieciešams uz sava datora uzstādīt maršrutēšanas programmu, kura šifre un atšifrē kā arī saspiež un atspiež datus un novirza tos lietotājiem I2P tīklā. Lai darboties ar tīmekļa vietnēm, kas strādā šajā I2P tīklā, nepieciešams nokonfigurēt pārlūkprogrammu, lai tā novirza HTTP paketes maršrutētājam, kas klausās noteiktu portu [14]. Lai vērsties pie ārējā Internet tīkla no I2P iekšienes, nepieciešams izmantot proxy serveri no I2P iekšienes (outproxy), kuru uz doto brīdi nav daudz [15]. Tāpat ir iespējams piekļūt iekšējām vietnēm, lietojot speciālu proxy serveri.

Sākotnēji tīkls tika projektēts ar pieņēmumu, ka visi starpmezgli ir kompromitēti un ļaunprātīgi, tādēļ pretdarbībai tika veikta virkne noteiktu aktīvu darbību [14].

Visas datu plūsmas tīklā tiek šifrētas ceļā no sūtītāja līdz pat seņēmējam [14]. Kopumā, datu nosūtīšanas laikā tiek izmantoti četri šifrēšanas līmeņi [14]. Pirmš šifrēšanas katrā paketē tiek ievietoti papildus lieki baiti, lai vēl vairāk padarīt nesaprotamu nododamo informāciju un apgrūtināt satura analīzes mēģinājumus kā arī nododamo pakešu bloķēšanas mēģinājumus [14].

Kā adreses tīklā tiek izmantoti kriptogrāfiskie identifikatori, kas pēc būtības ir atklātās kriptogrāfiskās atslēgas [14]. IP adreses I2P tīklā netiek izmantotas nekur un nekad [14], tādēļ noteikt kāda mezgla patieso adresi tīklā nav iespējams. Katra lietotne uz datora, izveido sev personisku šifrētu, anonīmu tuneli vai vairākus. Tuneļi pārsvarā ir vienvirziena – izejošajiem datiem savi, bet ieejošajiem savi tuneļi [14]. Noskaidros tuneļa virzienu, garumu kā arī tuneļa veidotājprogrammu ir ļoti grūti. Visas nododamās paketes parasti tiek izplatītas līdz mērķim pa dažādiem tuneļiem, kas padara bezjēdzīgus mēģinājumus noklausīties un analizēt ejošo datu plūsmu, izmantojot sniferus. Bez tā, notiek periodiska jau izveidoto tuneļu maiņa pret jauniem tuneļiem ar jauniem parakstiem un šifrēšanas atslēgām [14]. Apmēram reizi 10 minūtēs [14]. Nav nekādu iemeslu satraukties par to, lai lietojumprogrammas nodrošinātu sava tīkla trafika šifrēšanu. Ja eskistē neuzticība pret trafika šifrēšunu programmās ar aizvērtu pirmkodu, piemēram Skype, šo problēmu var risināt, lietojot IP-telefonijas programmas, piemēram Ekiga, kas nodod savu trafiku atklātā viedā [14]. Jebkurā gadījumā, I2P tīkls veiks četru līmeņu šifrēšanu visām paketēm un padarīs drošu visu datu nosūtīšanu un saņemšanu.

I2P tīklā visas paketes tiek nošifrētas sūtītāja pusē un tiek atšefrētas tikai pie saņēmēja, pie tam neviens no starpnieku mezgliem nevar partvert atšifrētus datus un neviens no starpniekiem nezin, kurš ir datu sūtītājs un kurš saņēmējs, jo iepriekšējais mezgls var tikpat labi būt sūtītājs kā staprnieks, kā arī nākamais var tikpat labi būt saņēmējs kā nākamais staprnieks. Nav iespējams, kādas lomas spēlē paketes ceļā iepriekšējais un nākamais mezgls kā arī nav iespējams noteikt vai nākamais mezgls apstrādāja paketi vai vienkārši nodeva to tālāk.

I2P tīklā, dažādos līmeņos un dažadiem protokoliem, tiek izmantotas sekojošas šifrēšanas un parakstīšanas metodes [14]:

- 256 bitu AES CBC režīmā ar PKCS#5
- 2048 bitu Elgamala shēma.
- 2048 bitu Difija-Helmana algoritms
- 1024 bitu DSA
- 256 bitu HMAC
- 256 bitu hešošana SHA256

I2P tīkls tikai aizsākts 2003. gadā ar merķi atbalstīt tos cilvēkus, kuri ir ieinteresēti rīkā, kas ļauj izplatīt informāciju bez cenzūras, anonīmi, veikt privātu komunikāciju [14]. I2P ir mēģinājums radīt drošu, decentralizētu, bojājumpiecietīgu tīklu ar nelielu atbildes laiku, ar anonimitātu, kā arī mērrogojamību. Galējais mērķis ir spēja funkcionēt pat grūtos apstākļos, atrodoties zem dažādu financiāli un politiski ietekmīgu organizāciju spiediena. Visi tīkla aspekti ir pieejami atklātā pirmkoda veidā un ir bezmaksas. Tas ļauj lietotājiem pārliecināties par to, ka programmatūra dara tieši to, kas ir solīts un ļauj trešo pušu izstrādātājiem uzlabot tīkla aizsardzību pret uzstājīgiem mēģinājumiem ierobežot brīvu komunikāciju.

I2P ir anonīma, vienranga, decentralizēta komunikāciju vide, ar kuru var strādāt ka tradicionālie tīkla pakalpojumi, tādi kā e-pasts, IRC, HTTP, Telnet, tā arī dažādi decentralizēti servisi, SQUID datu bāzes, DNS u.t.t [14, 15].

2.4.2. Netsukuku

Netsukuku ir decentralizēta, pašorganizējoša, vienranga tīkla radīšanas un izveidošanas projekts [16]. Tīkls varētu nodrošināt liela mezglu sakita mijiedarbību tajā pašā laikā veicot minimālu noslodzi uz procesoru un atmiņu. Šajā tīklā iespējams nodrošināt augstu bojājumpiecietību, anonimitātu, cenzūras neiespējamību un pilnu neatkarību no Internet tīkla [16,17].

Projekta pamatā ir ideja par plašām bezvadu tehnoloģijas iespējām: ja lietotāju datori darbosies kā maršrutētāji tīklā, tad iespējams izveiodt pašorganizētu tīklu uz to pamata, kurš teorētiski var būt daudz lielāks par Internet tīklu [16].

Netsukuku ir sietveida topoloģijas vienranga tīkls, kurš automātiski ģenerējas un patstāvīgi atbalstās. Tā ir radīta ar mērķi pārvaldīt neierobežotu mezglu skaitu ar minimāliem resursu tēriņiem. Pateicoties šim nākotnē būs iespējams uzbūvēt decentralizētu, anonīmu un nekontrolējamu vispasaules globālu tīklu atsevišķi un pilnīgi neatkarīgi no Internet tīkla, bez visādu dienestu atbalsta, bez pakalpojumu sniedzējiem un tamlīdzīgām ierobežojošam parādībām [17]. Tāds tīkls sastāv no datoriem, kas ir fiziski savienoti viens ar otru, tādeļ nav nepieciešamības izmantot jau esošas tīklu infrastruktūras [16]. Netsukuku rada tikai maršrutus, kas savieno datorus vienotā tīklā. Citiem vārdiem sakot, Netsukuku aizvieto 3. OSI modeļa līmeni ar citu maršrutēšanas protokolu [16].

Kā DNS aizvietotāju Netsukuku autori piedāvā lietot ANDNA (Abnormal Netsukuku Domain Name Anarchy) [16].

Netsukuku ir automātiski pārvaldāma. Tā rada pati sevi un var funkcionāt autonomi. Pievienojoties Netsukuku jaunam mezglam tīkla automātiski pārraksta sevi un visi pārējiem mezgli iegūst visātrāko un efektīvāko ceļu līdz jaunpievienotajam mezglam. Mezgli ir bez privilēģijā un ierobežojumiem salīdzinot ar citiem mezgliem [16], tie katra ir daļa no vienota tīkla.

Palielinoties mezglu skaitam, tīkla aug un kļūst arvien efektīvāks. Netsukuku nav starpības starp globālo un lokālo tīklu, tādēļ runāt par lokālo tīklu ir bezjēdzīgi.

Tāds tīkls nevar tikt kontrolēts vai izjaukts, jo tas ir pilnībā decentralizēts un sadalīts. Vienīgais veids, kā šādu tīklu iznīcināt ir izvest no ierindas katru tā mezglu vai arī sadalīt to nesavienotās saliņās [16].

Netsukuku tīklā jebkurš, jebkad un no jebkurienes var pieslēgties tīklam bez visādiem birokrātiskiem un tiesiskiem apgrūtinājumiem. Bez tam, katrs mazgls ir dinamisks un nepatstāvīgs. IP adrese, kas identificē datoru, tiem izvēlēta nejauši un to nevar saistīt ar reālu fizisku signāla atrašanās vietu [16]. Pie tam nav nekāda kontakta ar jebkādām organizācijām.

Tīkla caurlaidība tiek ierobežota tikai ar mūsdienu tīkla karšu iespējām.

Netsukuku ir sietveida topoloģijas tīkls, kas strādā ar maršrutēšanas protokolu Npv7_HT [16]. Jeb precīzāk runājot tika projektēts strādāt ar šo protokolu. Eskistē liels daudzums dinamiskās maršrutēšanas protokolu, bet tie visi atšķiras no dotā, jo pamatā tiek izmantoti nelielos tīklos. Internet pārbaldībā tiek izmantoti dažādi protokoli, to skaitā OSPF, RIP, BGP, kuru pamatā ir klasiski algoritmi, kas spēj atrast īsāko ceļu līdz mērķa mezglam. Dotie protokoli prasa lielus resursus no procesora un atmiņas savai izpildei. Tamdēļ šādu

uzdevumu veikšanai nepieciešamas speciālas iekārtas, neviens no šiem protokoliem nespētu radīt un uzturēt tādu tīklu kā Netsukuku, kurā katrs mezgls tiek pārvaldīts patstāvīgi, jo pilns maršrutu ceļš, ko būtu jāglabā uz katra datora prasītu apmēram 10 GB vietas [16].

Npv7 struktūra ir tīkls kā fraktālis [16]. Lai izskaitļot visus nepieciešamos mezgla sakaru kanālus ar visiem citiem mezgliem, protokols izmanto īpašu algoritmu, ko sauc par Quantum Shortest Path Netsukuku (QSPN) [16].

Fraktālis ir matemātiska struktūra, kurai piemīt rekursivitātes īpašība: katra tās daļa ir samazināta vesalā kopija, tādējādi iespējama stipra struktūras, kura var bezgalīgi izplesties, saspiešana. Tas nozīmē, ka ir nepieciešami tikai daži kilobaiti vietas, lai glabāt visu Netsukuku maršrutu karti. Maršrutu kartes struktūra var tikt definēta kā augsti klāsterizēts mezglu grafs.

No citas puses QSPN ir metaalgoritms tādā ziņā, ka neseko nekādiem matemātiskiem nosacījumiem, bet izmanto nejaušību un haosu, kuri neprasa sarežģītu skaitļošanu [16]. QSPN izpildās reālos tīklis, mezgli nosūta QSPN paketes, lai radīt tīklu. Šī iemesla dēļ ne vienmēr ir patiess apgalvojums, ka noteikta pakete tiks nosītīta ātrāk par kādu citu.

Netsukuku neierobežojas ar tīklu radīšanu, kas sastāv tikai no datoriem. Protokols var tikt izmantots jebkurā situācijā, kad nepieciešams savienot mezlgus savā starpā [16].

Mobilie telefonu tīkli principā ir tūkstošiem mezglu, kas savienoti vienā mezglā, kurš sadala trafiku un nodod informāciju Netsukuku mērķa mezglam, tas var tikt izmantots mobilajos telefonos, padarot, bezjēdzīgu daudzo mobilo sakaru operatoru eksistenci [16].

Netsukuku ir iespējams ieviest jekurās komunikāciju sistēmās, kas tiek izmantotas mūsdienās [16,17].

2.4.3. Hyperboria

Hyperboria principā turpina un attīsta tās idejas, kas tika izdomātas un mēģinātas realizēt Netsukuku ietvaros. Arī Hyperboria varētu strādāt bezvadu sietveida tīkla veidā un pasaulē ir vairākas šādas saliņas, taču ņemot vērā šobrīdējos apstākļus izveidot globālu nekontrolējamu jeb pašorganizējošos, decentralizētu sietveida tīklu nav iespējams, taču toties šīs saliņas ir iespējams tunelēti savienot caur Internet infrastruktūru [18,19].

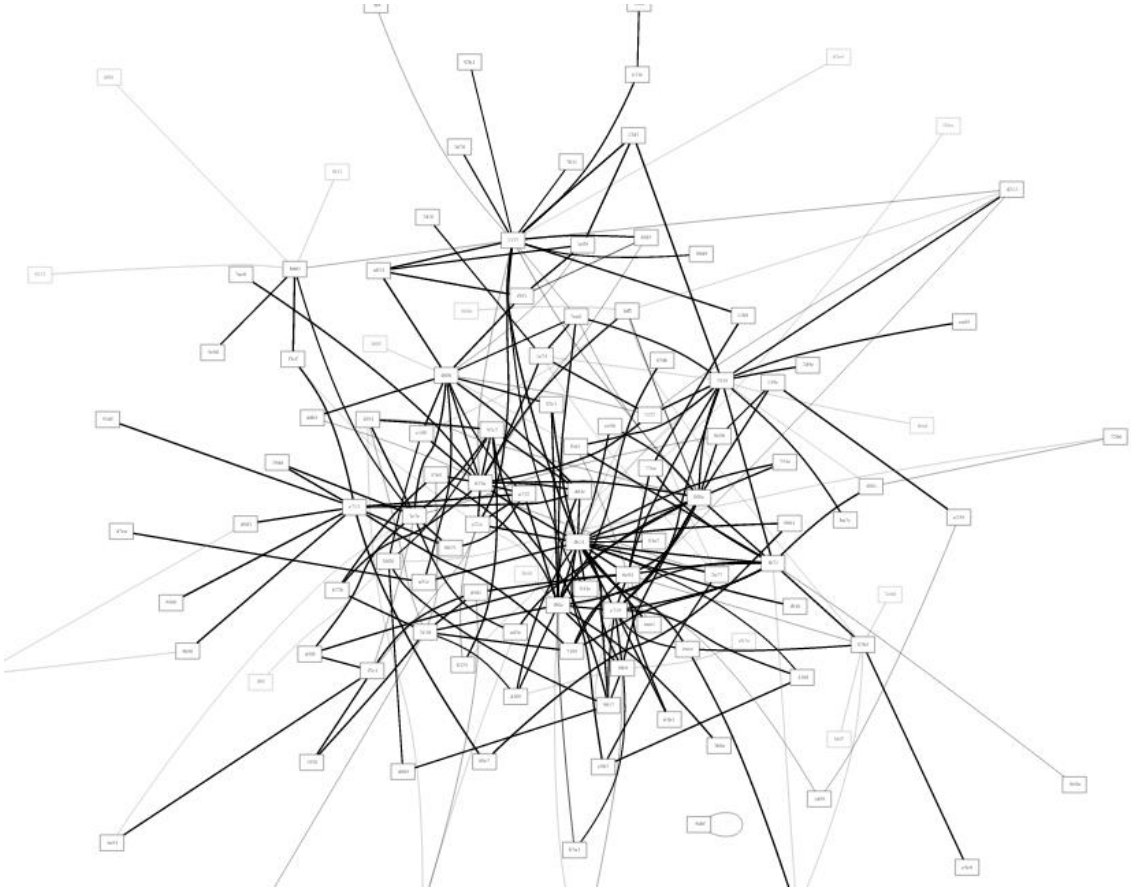
Tā kā Hyperboria tiks detalizēti analizēta un apskatīta atsevišķā nodaļā, kā arī tiks atsevišķi testēta un izmēģināta, tad šajā nodaļā dziļš apraksts netiks veikts.

Ir svarīgi piebilst, ka Hyperboria ir paredzēta darbam divos režīmos – kā bezvadu sietveida tīkls, tai skaitā globālos mērrogos, jo Hyperboria pamatā esjošais cjdns protokols ir

veiktspējīgs un viegls attiecībā pret resursparasībām, līdzīgi kā ar Netsukuku protokolu, taču Hyperboria ņemot vērā reālijas strādā arī pa virsu Internet tīklam un karts Internet tīkla lietotājs var kļūt par Hyperboria dalībnieku [19,20]. Kā tas tehniski notiek un kādas tam ir priekšrocības, tiks apskatīts trešajā nodaļā.

Uz doto brīdi Hyperboria tiek izmantota kā cjdns protokola testēšanas un izmēģināšanas platforma, taču tīklā ir apmēram 311 aktīvi mezgli un tīkls saturiski ir līdzīgs Internet tīklam tā attīstības sākumos. Ir vairākas vietnes, kurās nav reklāmu, daži bezmaksas servisi, piemēram e-pasts, failu glabātuve un daudzi personīgi blogi, pamatā veidoti šaurai auditorijai.

Attēlā 2.1. ir redzama Hyperboria tīkla karte vienā no tīkla attīstības etapiem. Kā redzams attēlā, tīkls vēl nav ļoti liels, taču lieliski redzams, ka tas ir sietveida un decentralizēts.



2.1. att. ***Hyperboria tīkla karte vienā no attīstības etapiem***

Hyperboria sniedz iespēju privāti un šifrēti nosūtīt datus, ja Hyperboria kļūtu par tikai bezvadu tīklu globālos mērrogos, tad tā varētu garentēt arī anonimitāti, taču mūsdienu Hyperboria tīkla mērķis [21] nav nodrošināt aninimitāti, bet gan sniegt privātumu, cīnīties pret cenzūru, dažādu komunikācijas ieribežošanu un ļaut testēt cjdns protokolu.

Potenciāli Hyperboria līdzīgi kā augstāk aprakstītais Netsukuku varētu kļūt par globālu sietveida tīklu, kurš pēc saviem izmēriem un efektivitātes pāraugtu Internet tīklu un būtu

brīvs, bez iespējamas cenzūras, praktiski neiznīcināms, bez iespējām to negatīvi ierobežot un ietekmēt no nelabvēlīgu, ietekmīgu organizāciju puses.

2.4.4 Salīdzinājums un secinājumi

Autors šīs apakšnodaļas ietvaros apskatīja iespējamos risinājumus, lai nodrošināt zināmā mērā vai pilnībā decentralizāciju, paaugstinātu bojājumpiecietību, privātumu un arī daļēji anonimitāti, kā arī izsargāties no cenzūras un dažādu iemeslu dēļ veicamiem mākslīgiem komunikācijas ierobežojumiem tīklā.

Apskatītie risinājumi nav vienīgie iespējamie, bet ir interesanti darba kontekstā, kura ietvaros tiek apskatīti sietveida tīkla darbības principi ar īpašu interese pret iespējām un mēģinājumiem veidot šāda veida globālu tīmekli.

Protams, apskatītais I2P risinājums nemaz nepretendē uz globāla fiziska sietveida tīkla realizēšanu, taču mūsdienu reālijās siendz privātuma un anonimitātes kā arī pretcenzūras iespējas un ar to ir interesants kā šībrīža praktisks risinājums.

Netsukuku ir bijis tiešs mēģinājums radīt autoru darba ietvaros interesējošu globālu bezvadu sietveida tīklu ar visām izrietošajām šāda nekontrolējama jeb pašorganizējoša tīkla īpašībām, taču projekts uz darba rakstīšanas brīdi neizrāda aktīvas dzīvības un atīstības pazīmes.

Hyperboria tīkls principā ir testa platofrma cjdns protokolam. Šis projekts attīsta tās idejas un principus, kas tika likti Netsukuku pamatā, taču atšķirībā no iepriekšminētā ir dzīvs, strādām tam var pieslēgties un notiek tā attīstība. Sakarā ar to, ka Hyperboria tīkls ir viens no tuvākajiem rezultātam risinājumiem, tas ir interesants autoram šī bakalaura darba ietvaros un tiks pētīts tuvāk.

Kopsavilkumā jāsaka, ka I2P ir labs esošs risinājums privātuma un anonimitātes nodrošināšanai, kurš strādā globāli un izmanto datu pārraudīšanai Internet tīklu. Autors uzskata par ļoti svarīgu privātumu, kura kā tāda Internet tīklā pēc noklusējuma principā nav un divējādi izturas pret aninimitāti, kas gan sniedz negatvīvu darbību veikšanas iespējas, to skaitā nelikumīgu, gan arī palīdz cīnīties pret ierobežojumiem un cenzūru. Autors uzskata, ka anonimitātes ētiskās puses jautājums ir risināms citā līmenī, ne šī darba ietvaros.

Netsukuku un Hyperboria tīkli ir tie, kas sniedz visdzīļāko interesi autoram, jo ir perspektīvi globāli bezvadu sietveida pašorganizējošies tīkli. Tā kā Netsukuku principā izskatās kā pamests projekts, tas īpašu interesi izraisa tieši Hyperboria.

Hyperboria jau pašreizējā formā sniedz sietveida pašorganizējošas tīkla priekšrocības un siendz privātuma nodrošināšanu, tiesa gan nav tik izplatīts un lietots kā I2P vai TOR

saprotamu iemeslu dēļ, to skaitā, jo nesniedz dotajā brīdī anonimitātes garantiju, kas nav starp tīkla radīšanas mērķiem un nav saprātīgi realizējams darbojoties pa virsu Internet tīklam, bet kļūs automātiski pieejams darbojoties tikai bezvadu fiziku svienojumu tīkla režīmā.

3. CJDNS PROTOKOLS UN HYPERBORIA TĪKLS

Šīs nodaļās ietvaros autors izskata Hyperboria tīklu un cjdns protokola darbību. Hyperboria tīkls izraisa paaugstinātu interesi bakalaura darba ietvaro kā vistuvākā uz doto brīdi pabeigtībai globāla sietveida pašorganizēta tīkla realizācija, kas joprojām tiek attīstīta un pat ir pieejama publiski un tiek salīdzinoši aktīvi lietota.

Nodaļas ietvaros ir paredzēts apskatīt cjdns un tīkla darbības koncepcijas un idejas kā arī pieslēgties Hyperboria tīklam un izmēģināt tajā sazināties ar citiem tīkla mezgliem un apskatīt kādā īsti stāvoklī ir tīkls.

Nodaļas ietvaros būs nepieciešams veikt atbilstošu iekārtu konfigurēšanu, kas arī tiks aprakstīts un veikt tīkla darbības testēšanu, kas arī tiks aprakstīts un, protams izpētī tīkla struktūru un pieslēgties kādam tīklā esošam pakalpojumam vai vairākiem.

3.1. Vispārejs apraksts un mērķi

Hyperboria ir decentralizēts vienranga tīkls, kurš būvēts uz cjdns maršrutēšanas dziņa. Tā tika radīta, lai jebkuri dati, kas tiek nosūtīti caur Internet tīklu tiktu droši nošifrēti un piekļuves ātrums pie datiem tiektos uz maksimāli iespējamo [7].

Pēc Hyperboria uzstādīšanas uz lietotāja datora tiek izveidots virtuāls tuneļa adapteris TUN0 [22]. Tam tiks piešķirta unikāla, nejauša IPv6 adrese, kuru nekādā veidā nebūs iespējams saistīt ar datora reālo IPv4 adresi. Tādā veidā, jubkura programma, kura spēj strādāt ar IPv6 protokolu, varēs strādāt Hyperboria tīklā [22].

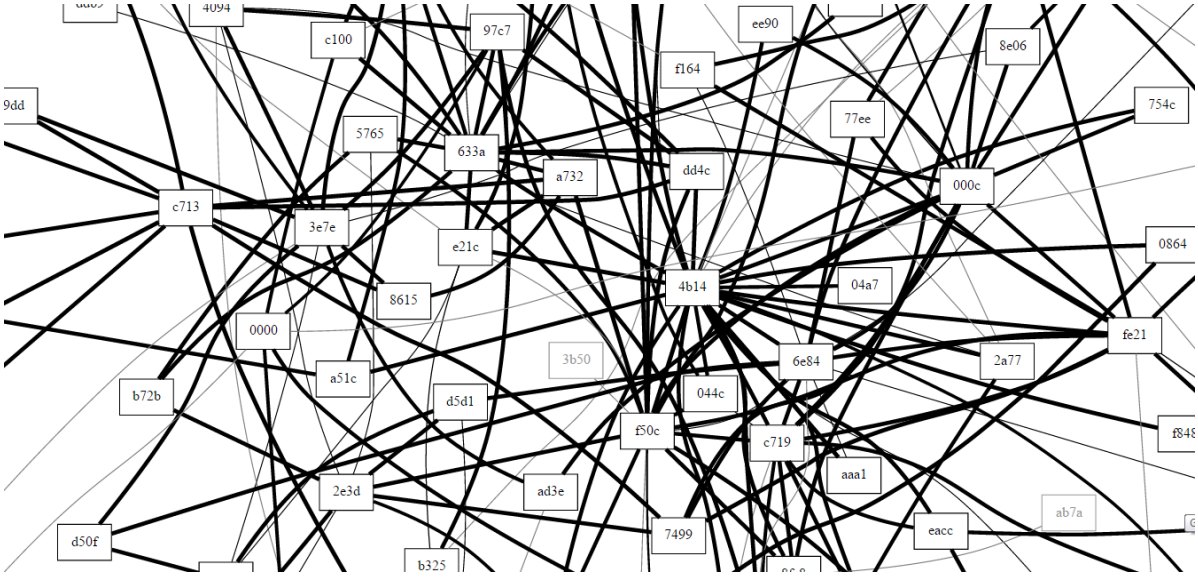
Hyperboria viens no izveides mērķiem ir sākotnēji radīt daudzas fiziskas bezvadu sietveida tīkla saliņas [21], kas strādā izmantojot cjdns protokolu saliņas un tad tās apvienot izmantojot tunelētu savienojumu caur Internet tīklu. Šads process varētu kalpot par pamatu tālākai tīkla izaugsmei globālā līmenī.

Lietotājiem, peislēdzoties tīklam nav jāsatraucas, ka pie viņiem ieradīsies policija un paziņos, ka izmantojot viņu mezglu ir uzlauzts kāda bankas sistēma, jo Hyperboria tīkls nav pieslēgts Internet tīklam un no Hyperboria tīkla nav iespējams pieslēgties Internet tīklam [19,20]. Tie ir divi dažādi tīkli, lai arī Hyperboria daļēji izmanto Internet fizisko infrastruktūru. Uz doto brīdi tas ir vienīgais veids kā tīklam būt globālam un vienotam.

Šis faktors gan ierobežo tīklu, gan arī tomēr sniedz lietotājiem ne tikai būt pieslēgtiem citā tīklā, bet arī ļauj nosūtīt šifrētus datus lietotājiem citā pasaules malā, kurus nav iespējams atšifrēt pārtverot vai pielietot tiem cenzūru, kā arī nav iespējams vienkārši bloķēt, jo nekontrolējama sietveida tīkla princips paredz plašu veidu ceļu, pa kuriem var tikt sūtīti dati

un bloķēt tos ir ļotī grūti un būtu neiespējami pilnvērtīga bezvadu sietveida tīkla gadījumā, par kādu perspektīvā varētu kļūt Hyperboria vai arī alternatīvs tīkls uz cjdns protokola bāzes.

Attēlā 3.1. ir redzams Hyperboria tīkla kartes fragments lielā tuvinājumā.



3.1. att. ***Hyperboria tīkla kartes fragments tuvinājumā***

Kā redzams šajā attēlā 3.1., tad katrs mezgls, kas ir apzīmēts ar baltu taisnstūri ar četru simblu virkni ir savienots ar daudziem citiem mezgliem. Četri simboli ir IPv6 adreses pēdējais bloks, pēc kura šajā kartē tiek indetificēti mezgli. Zamāk aprakstītā eksperimenta rezultātā par mezgliem tīklā kļūs arī divas autora darbstacijas.

3.2. Hyperboria darbība

Hyperboria ir vienranga tīkls, kurš spēj strādāt divos režīmos [18]:

1. Pa virsu Internet tīklam – overlay režīmā. Hyperboria strādā daudz ātrāk par Tor un I2P.
2. Tieša veidā starp maršrutētājiem, veidojot oriģinālu fizisku tīklu. Pamatā starp bezvadu maršrutētājiem.

Lai pieslēgties tīklam Hyperboria nepieciešams uzstādīt programmu, kas izpilda cjdns maršrutētāja lomu vai iegādāties nokonfigurētu cjdns maršrutētāju vai arī pārveidot par tādu savu maršrutētāju, uzstādot atbilstošu programmatūru un, pieslēdzoties, caur Internet tīklu [23], sameklēt jau eksistējošu Hyperboria mezglu un uzzinot tā adresi un atslēgu [24], pieslēgties tam [23]. Pieslēgties var, saprotams, vairākiem mezgliem un izmantot sietveida topoloģijas priekšrocības. Bet pieslēdzoties fiziskā Hyperboria segmentā no maršrutētāja pie maršrutētāja viss notiks automātiski [22].

Pēc pieslēgšanās tīklam, visi nosūtītie dati tiks šifrēti un atšifrēt tos varēs tikai saņēmējs. Datus nebūs iespējams pārtvert un izlasīt vai veikt cenzūru [18,19].

Šifrēšanas mehānisms realizēts izmantojot mezglu privātās un publiskās atslēgas, kas garantē drošību, pie nosacījuma, ka privātās atslēgas ir neaizskaramas un labi nosargātas [20].

3.3. Maršrutēšana tīklā

Tīkla katram mezglam tiek ģenerēta IPv6 adrese, kura attiecas IPv6 privātajam adrešu sektoram, un tātad nenotiks kolīzijas starp īsto IPv6 tīklu un Hyperboria tīklu.

Tīklā var darboties jebkura lietotne, kas atbalsta IPv6. Pēc tam, kad tiek uzstādīta atbilstoši nepieciešamā darbam tīklā programmatūra, viss trafiks, kas domāts Hyperboria tīklam tiek automātiski novirzīts pareizajā virzienā un nav nepieciešams manuāli konfigurēt katru lietotni vai sistēmu.

Datu plūsmu maršrutēšana notiek izmantojot sistēmu, kura ir analoģiska Kademlia DHT sistēmai, precīzi runājot maršrutu katalogs tiek pastāvīgi atjaunots, ja notiek izmaiņas tīkla konfigurācijā, tādā veidā tīkls uztur optimālu noslodzi visiem mezgliem un tiek izvēlēts visīsākais ceļš datu nosūtīšanai.

3.5. Anonimitāte un privātums

Hyperboria ir privāts tīkls – nosūtītās datu plūsmas tiek šifrētas un var tikt atšifrētas tikai saņēmēja iekārtā. Tiek izmantota publiskās un privātās atslēgas šifrēšana.

Tīkls nav anonīms. Hyperboria radīšanas mērķis nebija izveidot I2P vai Tor klonu, bet gan veidot jaunu internetu [21]. Ar trasēšanas palīdzību ir iespējams iegūt mezglu virknīti un uzzināt iekārtas atrašanās vietu kamēr vien notiek darbošanās pa virsu Internet tīklam. Saprotams, ka tiklīdz notiek darbošanās tikai stapr fiziski bezvadu vidē savienotām iekārtam pilnvērtīgā ebzvadu sietveida tīklā, tā automātiski tiek nodrošināta arī anonimitāte [18,19]. Kā arī būtu jābūt pašorganizējošā, decentralizētā, sietveida bezvadu tīklā.

3.6. DNS

Dotajā brīdī Hyperboria tīklā strādā klasiska DNS realizācija, taču notiek jaunas decentralizētas DNS sistēmas izstrāde, kas nomainīs klasisko centralizēto risinājumu [7].

Eksistē un tiek attīstīti vairāki decentralizēta DNS radīšanas projekti, tādi kā DIANNA, DIANNA2, Namecoin, Nxt, Emercoin un citi [7].

3.7. Pieslēgšanās tīklam un testēšana

Lai izmēģināt pieslēgties Hyperboria tīklam, autors nolēma izmantot Linux Mint 17.1 Rebecca operētājsistēmu un nepieciešamās programmatūras uzstādīšanu tajā, lai pieslēgties tīklam caur Internet pieslēgumu. Diemžēl Latvijā nav izveidots fizisks Hyperboria segments, kuram varētu mēģināt pieslēgties izmantojot maršrutētāju, tādējādi kļūstot par pilnvērtīgu tīkla dalībnieku fiziskā līmenī. Bet tā vietā tiks izmēģināts tīkls overlay režīmā.

Uzstādīšanas process kā arī tīkla izmēģināšana ir detalizēti aprakstīta šajā nodaļā.

3.7.1. Testēšana plāns

Autors plāno pieslēgties Hyperboria tīklam no diviem dažādiem datoriem, kuri tiks implementēti testā kā virtuālās mašīnas uz viena fiziska datora. Abas virtuālās mašīnas ar Linux Mint 17.1 operētājsistēmu tiks pieslēgtas vienam lokālam tīklam ar fizisko datoru, uz kuras tās atrodas un tiks kā divi dažādi datori autonomi pieslēgti Hyperboria tīklam.

Uz viena no datoriem ir paredzēts uzstādīt pulbiski pieejamu web-serveri un paredzēts no otra datora pieslēgties tam. Ņemot vērā, ka lai arī abas mašīnas būs vienā lokālajā tīklā, tomēr no Hyperboria viedokļa, tās abas tiks tieši pievienotas globālajam tīklam un katrai no tām tiks piešķirta sava pilnvērtīga Hyperboria tīkla IPv6 adrese.

Ir paredzēts pieslēgties arī jau esošiem tīmekļa serveriem Hyperboria tīklā.

Lai pieslēgties Hyperboria tīklam, ir paredzēts izmantot publiskos pieslēgšanās mezglus Internet tīklā.

3.7.2. Uzstādīšana un iestatīšana

Šajā apakšnodaļā aprakstītais uzstādīšanas process un aprakstītas komandrindas komandas atbilst Linux Mint 17.1 operētājsistēmai. Citām sistēmām procesa būtība, protams, ka saglabāsies, bet pielietojamās komandas var atšķirties.

Lai pieslēgties Hyperboria tīklam, vispirms nepieciešams uzstādīt operētājsistēmā cjdns realizāciju. Tas nepieciešams, lai operētājsistēma varētu strādāt ar cjdns protokolu. Lai to izdarīt, nepieciešams lejuplādēt cjdns realizācijas kodu un nokompilēt to.

Linux Mint 17.1 operētājsistēmā nepieciešams uzstādīt kompilēšanas rīkus. Tas paveicams ar sekojošu komandu, kas jāieraksta terminālī jeb konsolē:

```
sudo apt-get install nodejs git build-essential
```

Uzstādīt *nodejs* paketi nav obligāti, bet ir vēlams to izdarīt uzreiz.

Cjdns realizācija ir pilnībā atvērta koda [23,24]. To ir iespējams lejuplādēt no git repozitorija, Linux Mint 17.1 operētājsistēmā, izmantojot komandu:

```
git clone https://github.com/cjdelisle/cjdns.git cjdns
```

Lai veikt tālākās darbības veidā, kā aprakstīts turpmākajā aprakstā, nepieciešams atrasties tikko radītajā *cjdns* direktorijā. To var izdarīt, pielietojot komandu:

```
cd cjdns
```

Tālāk nepieciešams veikt koda kompilāciju. Tas paveicams, atrodoties cjdns direktorijā, kas piepildīta ar git repozitorija saturu un veicot komandu:

```
./do
```

Nepieciešams saigaidīt līdz paradīsies paziņojums par veiksmīgu kompilāciju. Tas izskatīsies šādi:

```
Build completed successfully, type ./cjdroute to begin setup.
```

Tālākajās darbībās notiek cjdns realizācijas uzstādīšanas pabeigšana un konfigurēšana sistēmā. Lai uzstādīt cjdns uz Linux Mint 17.1, nākamais veicamais solis pēc kompilācijas ir pārliecināšanās par to, ka viss ir paveikts pareizi. Ir nepieciešams palaist cjdns bez parametriem izpildot komandu:

```
./cjdroute
```

Pēc šīs komandas izpildes terminālī tiks izvadīta informācija un iespējamie darbību varianti.

Principā uzstādīšana ir praktiski pabeigta, atliek tikai nokonfigurēt cjdns, lai varētu pieslēgties Hyperboria tīklam. Lai uzģenerēt konfigurācijas failu, jāizpilda komanda:

```
./cjdroute --genconf >> cjdroute.conf
```

Tālāk, nepieciešams atrast kādu mezglu Hyperboria tīklā, kuram varētu pieslēgties [23]. Kā jau tika runāts iepriekš darbā, Hyperboria tīkls ir vienranga, pašorganizējošs sietveida tīkls. Arī darbojoties pa virsu Internet tīklam, šī shēma loģiskā līmenī ir tāda pati.

Par šādu Hyperboria mezglu, caur kuru pieslēgties tīklam var kalpot jebkurš dators vai maršrutētajs šajā tīklā. Taču eksistē arī publiski pieejami pieslēgšanās mezgli.

To adreses ir apskatāmas un publiski pieejamas tīmekļa vietnē [23]. Autors nolēma nokonfigurēt pieslēgšanos veirākiem publiskiem mezgliem. Lai to paveikt nepieciešams rediģēt tikko uzģenerēto konfigurācijas failu. Attēlā 3.2. redzams konfigurācijas faila „connectTo” sadaļa pēc trīs Hyperboria publisko pieslēgšanās mezglu iestatīšanas.

```
        // Nodes to connect to (IPv4 only).
        "connectTo":
        {
            "95.85.46.74:47670":
            {
                "password": "freedomforallmlzb0mnd9kyz1rnall",
                "publicKey": "guqq5h8p9w6mtxfuh1k9hl1yqljpqqnvj2umcd1cuvx64vbuqhu0.k"
            }
            "83.137.52.57:31337":
            {
                "password": "cjdnsDotixDotgs",
                "publicKey": "pvtgk72f25urxqywxdzfk12t2b4kuhtrc2f1mx58rtpx0wzbll90.k"
            }
            "82.146.34.103:63336":
            {
                "password":"vmtgs8phs8w7t76q3zr8v7nxr4txwd1",
                "publicKey":"h8p5609d03yt1fzu3dlky3g1kt3bq8gffhnsbq2z1dg8j46rt4w0.k"
            }
        }
    },
```

3.2. att. ***Cjdns publisko mezglu iestatīšana konfigurācijas failā***

Pēc tam, kad konfigurācijas fails tiek saglabāts, nepieciešams startēt cjdns servisu. Bet pirms tam, nepieciešams apzināties, ka dators kļūs publiski tieši pieejams no Hyperboria tīkla. Tam būs sava IPv6 adrese, kuru varēs tieši sasniegt jebkurš Hyperboria mezgls [24]. Arī gadījumos, kad dators atrodas kādā lokālā tīklā aiz ārējiem maršrūtētājiem, jo priekš Hyperboria tīkla šo ārejo maršrutētāju nav un dators tiks pieslēgts pa tiešu šajā piemērā trim nokonfigurētajiem mezgliem ar tunelētu savienojumu. Sakarā ar to, ir nepieciešams pārliecināties ka visi svarīgie pakalpojumu ir atbilstoši droši konfigurēti un datoram nav iespējams nodarīt kaitējumu vai nesankcionēti pieslēgties no Hyperboria tīkla [23].

Nākamais solis ir ieslēgt cjdns protokolu un maršrutēšanu un pieslēgties tīklam. Tas paveicams ar komandu:

```
sudo ./cjdroute < cjdroute.conf
```

Vai arī, ja ir nepieciešamība vai vēlme pēc log faila ar komandu:

```
sudo ./cjdroute < cjdroute.conf > cjdroute.log
```

Pēc šī soļa, ja ievadīt komandu:

```
ifconfig
```

būs redzams, ka pie esošajām tīkla saskarnēm ir parādījusies jauna – virtuāla `tun0` saskarne. Un šai saskarnei piemīt IPv6 adrese. Autora gadījumā tā bija `fccc:a26d:413a:bc96:e410:9d90:4012:dc91/8`. Ar šo adresi dators tagad ir pieejams no Hyperboria tīkla.

Pieslēgšanās ir pabeigta. Lai apstādināt cjdns un respektīvi atslēgties no tīkla, pietiek izpildīt komandu:

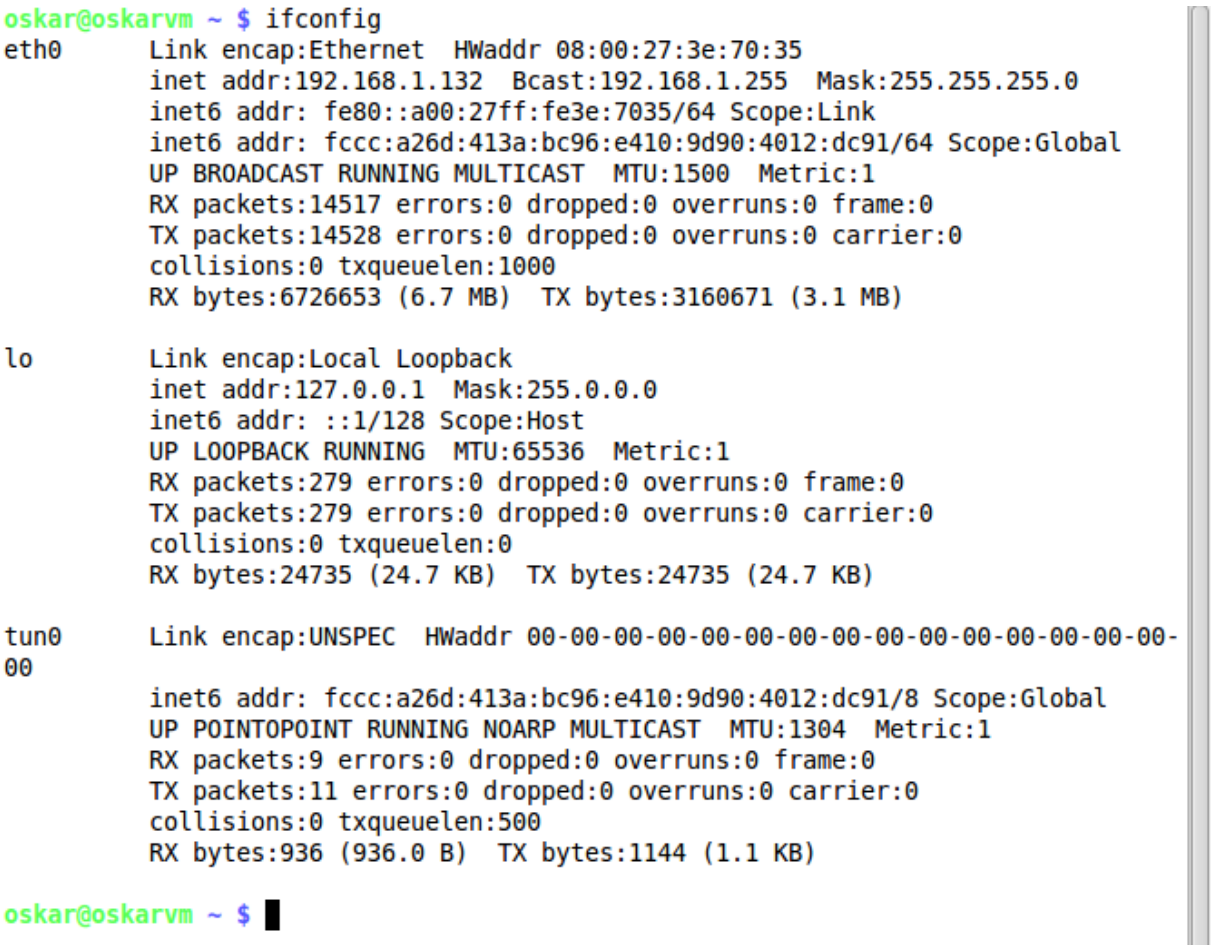
```
sudo killall cjdroute
```

Nākamajā apakšnodaļā tiks aprakstītas autora tālākās darbības tīkla testēšanā. Līdzīgā veidā autors pieslēdza Hyperboria tīklam divas Linux Mint 17.1 darbstcijas.

3.7.3. Testēšana un lietošana

Tikko kā uzstādīšana tika pabeigts, Hyperboria mezgli tika iestatīti un cjdns ir iespējots parādās jauns tīkla interfeis `tun0`, kuram jau ir piešķirta Hyperboria tīkla IPv6 adrese. Autors atgādina, ka Hyperboria tīklā mezgliem tiek piešķirtas adreses no tā sauktā privātā adrešu sektora jeb Unique Local Addresses (ULAs) [25]. Šis sektors ir paredzēts iekšējiem lokālajiem, jeb globāli nemaršrutējamajiem tīkliem [25]. Mūsdienu Hyperboria izmanto šīs adreses, lai izvairītos no kolīzijām ar reālām IPv6 adresēm un nebūtu problēmu mezgliem strādāt gan Internet tīklā, gan Hyperboria tīklā vienlaicīgi [18,19]. Kolīzijas var rasties, piemēram mēģinot pārlūkprogrammā atvērt kādu tīmekļa serveria ar IPv6 adresi, kurš atrodas Internet tīklā un citu serveri ar tādu pašu adresi Hyperboria tīklā. Tas varētu neizdoties. Taču šī problēma ir novērsta. Jāsaka gan, ka kolīzijas ar kādu potenciālu lokālu tīklu, kurš izmanto IPv6 var gadīties, un tādēļ ir nepieciešama šadā situācija papildus konfigurācija. Bet par to citviet.

Attēlā 3.3. un attēlā 3.4. ir redzamas abas autora darbstacijas, precīzi runājot atvērti tajās termināļi ar izpildītu komandu ifconfig, kura demonstrē veiksmīgu cjdns iespējošanu un adreses iegūšanu Hyperboria tīklā.



3.3. att. ***Jaunais tun0 interfeis un IPv6 adrese Hyperboria tīklā pirmajai darbstacijai***

Kā redzams šajā attēlā 3.3., tad pirmajai darbstacijai tīklā Hyperboria ir piešķirta IPv6 adrese `fccc:a26d:413a:bc96:e410:9d90:4012:dc91`.

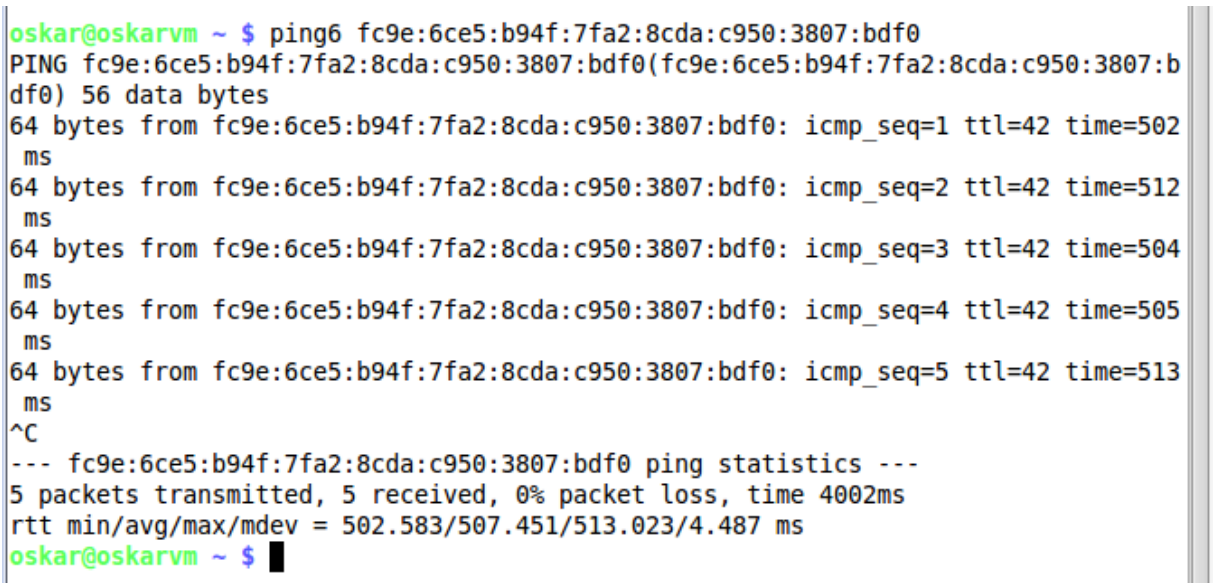
```
oskar@oskarVMTest ~ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0a:7d:5b
          inet addr:192.168.1.139  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0a:7d5b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16312 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16193 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6662596 (6.6 MB)  TX bytes:3902883 (3.9 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:247 errors:0 dropped:0 overruns:0 frame:0
          TX packets:247 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21173 (21.1 KB)  TX bytes:21173 (21.1 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-
00
          inet6 addr: fc9e:6ce5:b94f:7fa2:8cda:c950:3807:bdf0/8 Scope:Global
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1304  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:1664 (1.6 KB)  TX bytes:1976 (1.9 KB)

oskar@oskarVMTest ~ $
```

3.4. att. ***Jaunais tun0 interfeis un IPv6 adrese Hyperboria tīklā otrajai darbstacijai***

Kā redzams šajā attēlā 3.4., tad otrajai darbstacijai tīklā Hyperboria ir piešķirta IPv6 adrese fccc:a26d:413a:bc96:e410:9d90:4012:dc91.

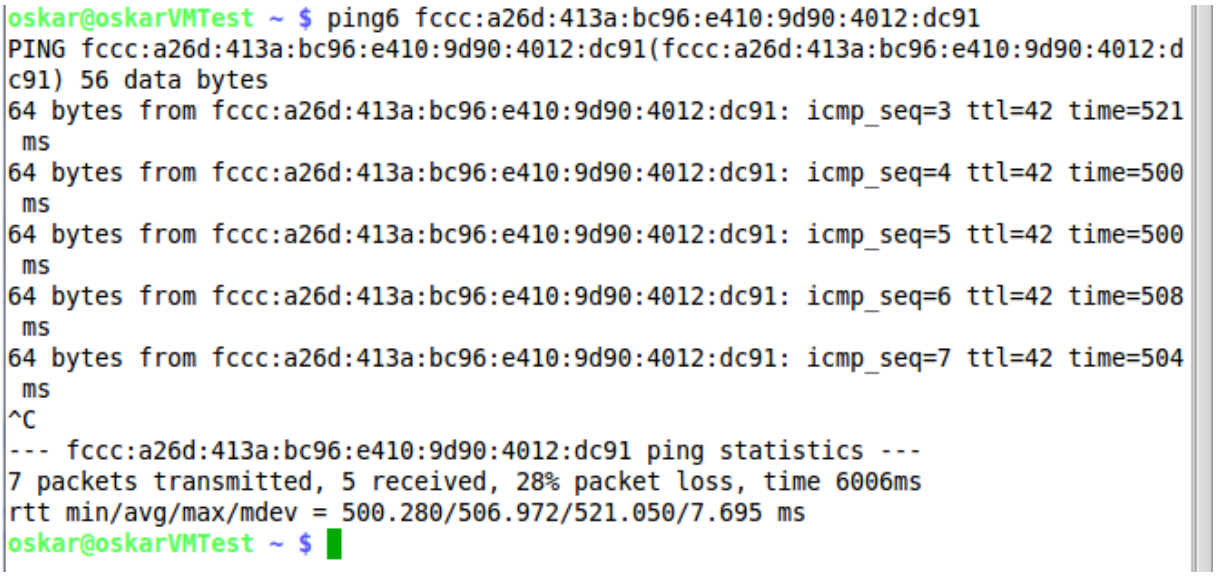
Pēc abiem attēliem var secināt, ka abas darbstacijas patiešām ir vienā lokālā tīklā, bet Hyperborias skatījumā tās ir atsevišķi, pilnvērtīgi tīkla mezgli pa tiešu ceļu pieejami no Hyperboria tīkla katrs ar savu personīgo, pilnvērtīgu tīkla IP adresi.

Attēlos 3.5. un 3.6. ir redzams, kā no vienas darbstacijas tiek pingota otra un otrādi. Tas ļauj pārliecināties par to, ka abas darbstacijas ir veiksmīgi pieslēgušās vienotam Hyperboria tīklam un ir savienojamas.



3.5. att. ***Otrās darbstacijas pingošana no pirmās darbstacijas caur Hyperboria tīklu***

Kā redzams šajā 3.5. attēlā, tad vidēji ping sigāls veic savu ceļu 507,451 milisekundēs, kas liek domāt, ka signāls patiešām ceļo caur kādu no pieslēgšanās tīklam mezgliem, kuri atrodas viens Amsterdamā un divi citi Maskavā [23], nevis kādā citā veidā pa taisno caur lokālo tīklu. Tā tam arī būtu jābūt, jo konfigurācijas failā katrai darbstacijai nav norādīts, ka tai ir jābūt pieslēgtai tīklam caur otru darbstaciju vai otrādi.



3.6. att. ***Pirmās darbstacijas pingošana no otrās darbstacijas caur Hyperboria tīklu***

Kā redzams šajā 3.6. attēlā, tad veicot pirmās darbstacijas pingošanu no otrās, vidējais signāla laiks ir aptuveni tāds pats. Tā tam arī būtu jābūt, ņemot vērā ka šī pingošana tika veikta tūlīt pēc tam un konfigurācija netika mainīta. Secinājums ir tāda, ka šobrīd tīklam ir pieslēgtas abas darbstacijas korekti un savienojums ir nostabilizēts.

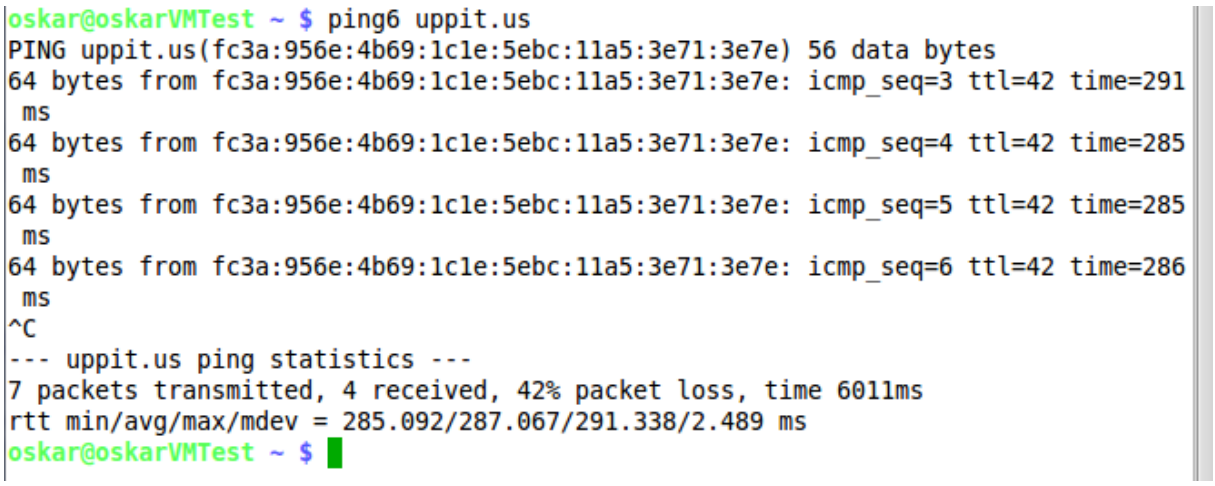
Nākamajos attēlos 3.7. un 3.8. ir redzams, kā tiek pingots attālināts serveris Hyperboria tīklā ar domēna vārdu uppit.us [26] no abām darbstacijām.

```
oskar@oskarvm ~ $ ping6 uppit.us
PING uppit.us(fc3a:956e:4b69:1c1e:5ebc:11a5:3e71:3e7e) 56 data bytes
64 bytes from fc3a:956e:4b69:1c1e:5ebc:11a5:3e71:3e7e: icmp_seq=4 ttl=42 time=352
 ms
64 bytes from fc3a:956e:4b69:1c1e:5ebc:11a5:3e71:3e7e: icmp_seq=5 ttl=42 time=332
 ms
64 bytes from fc3a:956e:4b69:1c1e:5ebc:11a5:3e71:3e7e: icmp_seq=6 ttl=42 time=350
 ms
64 bytes from fc3a:956e:4b69:1c1e:5ebc:11a5:3e71:3e7e: icmp_seq=7 ttl=42 time=316
 ms
64 bytes from fc3a:956e:4b69:1c1e:5ebc:11a5:3e71:3e7e: icmp_seq=8 ttl=42 time=382
 ms
^C
--- uppit.us ping statistics ---
8 packets transmitted, 5 received, 37% packet loss, time 7027ms
rtt min/avg/max/mdev = 316.328/346.604/382.156/22.078 ms
oskar@oskarvm ~ $
```

3.7. att. ***Attālināta servera Uppit.us pingošana Hyperboria tīklā no pirmās darbstacijas***

Kā redzams attēlā 3.7., tad dažas no nosūtītajām paketēm ir pazaudētas, kas ir saistīts ar nenoskaidrotiem apstākļiem. Taču ir korekti noteikts, kurā tīklā atrodas adrese un noteikta pati adrese domēna vārdam. Pings vidēji ceļo 346 milisekundes, kas ir labāk nekā nedaudz iepriekš pingojot darbstacijas savā starpā.

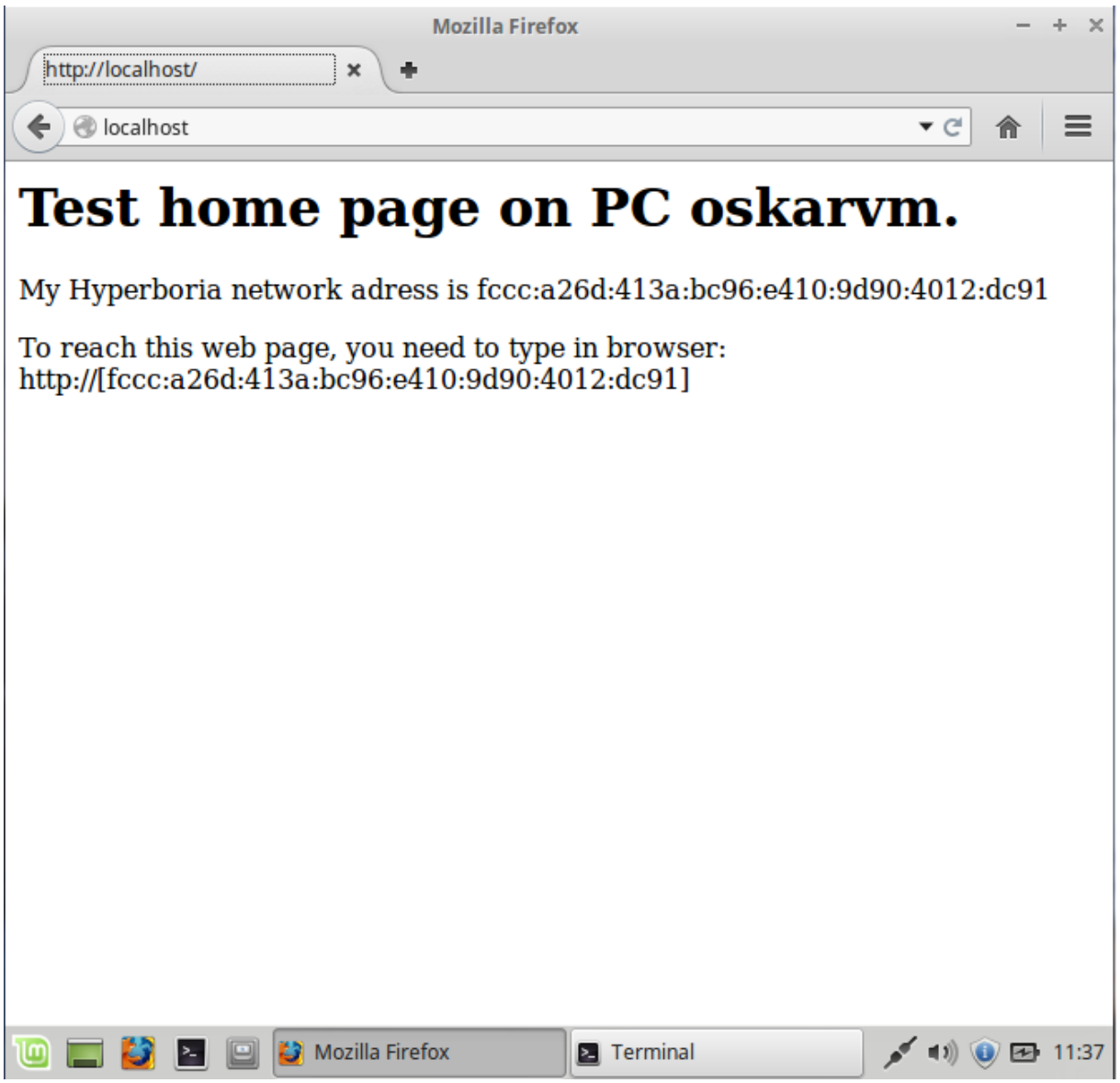
Domājams, tas ir saistīts ar to ka savienojums starp uppit.us serveri un kādu no pieslēgšanās punktiem ir ievērojami labāks nekā starp darbstaciju un pieslēgšanās punktu, jo izskatās, ka veikt ping pakates ceļu no darbstacijas līdz pieslēgšanās punktam, tad uz otru darbstaciju un atpakaļ ir nedaudz mazāk kā divas reizes ilgāk par ceļu no darbstacijas līdz pieslēgšanās punktam un tad līdz uppit.us serverim un atpakaļ, kas liek secināt, ka ja ceļš no darbstacijas līdz pieslēgšanās punktam varētu būt 125 milisekundes, tad līdz uppit.us serverim tas varētu būt 5 reizes mazāks. Bet tas nav būtiski, galvenais, ka ir nodibināts savienojums.



3.8. att. ***Attālināta servera Uppit.us pingošana Hyperboria tīklā no otrās darbstacijas***

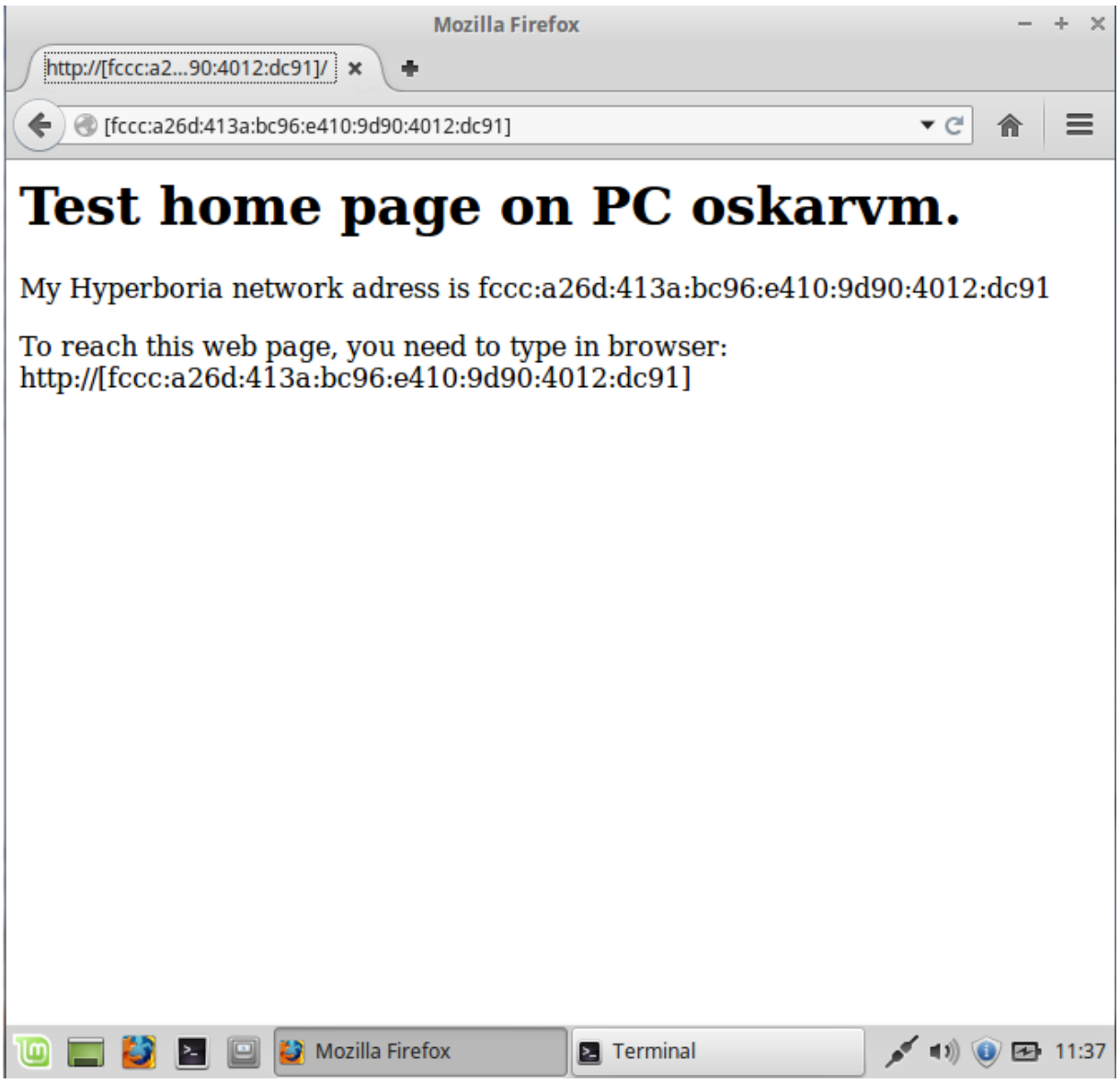
Kā redzams attēlā 3.8., tad dažas no nosūtītajām paketēm ir atkal pazaudētas, taču arī šis savienojums ir nodibināts.

Nākamajos attēlos 3.9. un 3.10. ir parādīta pieslēgšanās tīmekļa vietnei, kas ir iavietota uz pirmās darbstacijas. Pieslēgšanās notiek caut Hyperborie tīklu. Vispirms notiek vietnes darba pārbaude, pieslēdzoties tai no lokāli, pēc tam notiek pieslēgšanās caur Hyperboria tīklu no otras darbstacijas.



3.9. att. ***Pieslēgšanās pirmās darbstacijas tīmekļa serverim no pašas pirmās darbstacijas***

Kā redzams attēlā 3.9., tad vietne ir veiksmīgi iespējota un lokāli tai ir iespējams veiksmīgi pieslēgties.



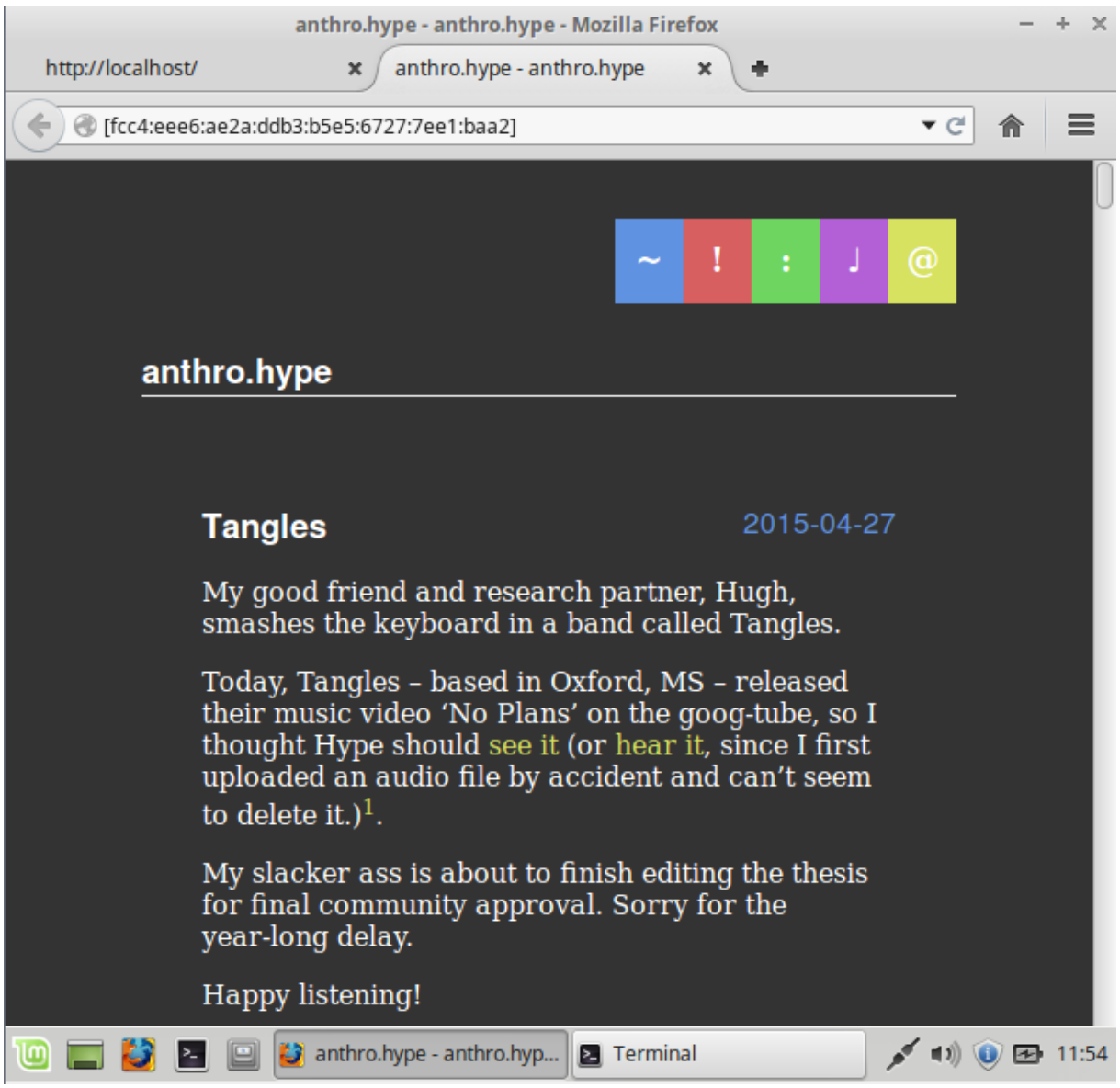
3.10. att. ***Pieslēgšanās pirmās darbstacijas tīmekļa serverim no otrās darbstacijas caur Hyperboria tīklu***

Kā redzams 3.10. attēlā, tad vietnei ir izdevies veiksmīgi pieslēgties arī caur Hyperboria tīklu no otras darbstacijas. Kā var saskatīt pārlūkprogrammas adreses joslā, tad tur ir ierakstīta pirmās darbstacijas adrese Hyperboria tīklā. Tā ir:

```
http://[ fccc:a26d:413a:bc96:e410:9d90:4012:dc91]
```

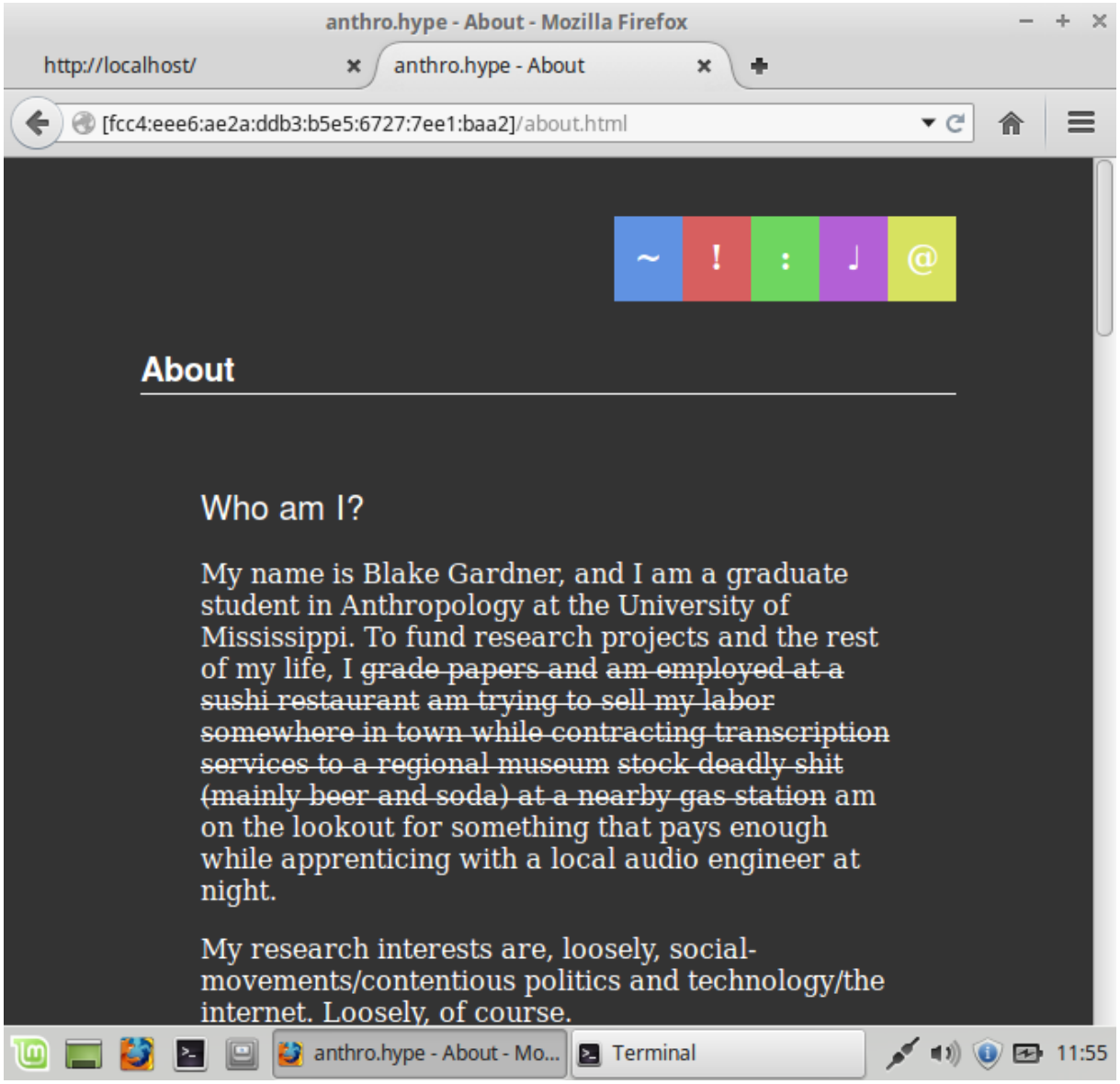
Šādā formā to jāieraksta pārlūkprogrammā, lai veikt pieslēgšanos uz darbstacijas esošajam tīmekļa serverim.

Nākamajos attēlos 3.11. un 3.12. ir redzams kā tiek veikts pieslēgums attālinātai tīmekļa vietnei [26] Hyperboria tīklā no pirmās darbstacijas.



3.11. att. ***Pieslēgšanās attālināta servera tīmekļa vietnei Hyperboria tīklā caur pārlūkprogrammu***

Kā redzams šajā attēlā 3.11. attālinātajai tīmekļa vietnei anthro.hype ir izdevies pieslēgties un tā veiksmīgi strādā Hyperboria tīklā.



3.12. att. ***Navigācija pa attālināta servera tīmekļa vietni Hyperboria tīklā caur pārlūkprogrammu***

Šajā attēlā 3.12. ir redzams, ka ir veiksmīgi veicama navigācija šajā tīmekļa vietnē gluži kā jebkurā tīmekļa vientē Internet tīklā.

Šis bija pēdējais testēšanas elements. Beigās nepieciešams teikt, ka Hyperboria tīklā kopumā strādā apmēram 311 aktīvu mezglu un principā ir izdevies nodibināt savienojumus ar dažiem no tiem kā arī ir izdevies pievienot tīklam divus autora mezglus, no kuriem uz viena strādā tīmekļa vietne, kuru var sasniegt jebkurš Hyperboria tīkla lietotājs.

3.8. Priekšrocības un trūkumi

Kopvērtējumā autors uzsver tās priekšrocības, ko dod un vēl spētu dot Hyperboria tīkls un cjdns protokols realizēts šādā veidā un pilnā apjomā, kā paredzēts, kā arī apzinās grūtības, kas saistīas ar tā realizēžanu un arī zināmus trūkumus šādai koncepcijai.

Hyperboria tīkls savā šobrīdējajā stāvoklī, darbojoties divos režīmos – pa virsu Internet tīklam un fiziskā līmeni starp atbilstošiem maršrutētājiem daudzās vietās lokāli, var sniegt zināmas priekšrocības, starp tām, pilnvērtīga privātuma aizsardzība – visi dati, kas tiek nosūtīti, tiek šifrēti un ir atšifrējami tikai uz adresāta iekārtas, jo tiek izmantota publiskās un privātās atslēgas šifrēšana.

Bez tā, jau šobrīd jebkurš, kurš vēlas var izvietot pilnībā bezmaksas Hyperboria tīklā savu tīmekļa serveri ar jebkādiem pakalpojumiem, jo Hyperboria tīkls ir pašorganizējošs un nekontrolējams – katrs ir pats sev pakalpojumu sniedzējs un automātiski, pieslēdzoties tīklam iegūst pilnvrtīgu adresi bez dažādu institūciju staprniecības un ir ar šo adresi sasniedzams no tīkla, sekojoši, ir iespējams ieveidot šīs adreses galā jebkādus nepieciešamus pakalpojumus. Vispopulārākais uz doto brīdi pakalpojums Hyperboria tīklā – ir personīgā tīmekļa vietne.

Tīkla izplatīšanās gadījumā, protams, tiktu daudz izteiksmīgāk redzamas tās sietveida topoloģijas priekšrocības, kas, jau ir, bet pieaugot tīkla kļūtu spēcīgākas. Pirmkārt, protams, bojājumpiecietība, kas nodrošina tīkla nepārtrauktu pieejamību jebkuram mezglam, pat ja kāds tam pievienots mezgls iziet no ierindas, jo eksistē vairāki ceļi, kā savienoties ar citām iekārtām.

Bez šaubām, ja tīkls kļūtu ļoti liels un tas darbotos pilnībā fizikā līmenī – ar savienojumiem stapr reālām iekārtām nevis tuneļiem caur Internet tīklu, tad tīkls būtu gan anonīms, kas vēl nav tik būtiski, gan, kas ir ļoti būtiski, visiem pieejams pilnībā bez maksas un jebkādiem birokrātiskiem šķēršļiem un pilnībā bez cenzūras vai mākslīgiem komunikāciju ierobežojumiem, jo kontrolēt un ierobežot sietveida pašorganizējošos bezvadu tīklu nav praktiski iespējams.

Tiesa situācijā, kad katrs ir pats sev pakalpojumu siendzējs un eksistē augsta līmeņa anonimitāte, ir problēmas kontrolēt, kā tiek izmantots tīmeklis, un to ir vieglāk lietot pretsabiedriskos veidos. Šis ir blakusjautājums, kurš palielina gan sabiedrības atbildību gan dažādu tīmekļa vietņu atbildību par sava satura paškontroli.

Par trūkumu ir uzskatāma arī neiespējamība nevienam garantēt noteiktu savienojuma ātrumu un stabilas aiztures. Savienojumi starp mezgliem var būt pilnīgi dažādi, tie var pārtrūkt un radīt kādas aiztures. Šīs ir nopietnas problēmas īpaši pakalpojumiem, kuru sniegšanai nepieciešams garantēts savienojuma ātrums un nav pieļaujamas lielas un nestabilas aiztures, piemēram straumēšana, tiešsaistes datorspēles un citas akcijas.

Ja runāt par drošību, tad gan satraukties nav par ko, jo, ja vien privātā mezgla atslēga nav kļuvusi pieejama nesankcionētām personām, tad datus, kad domāti konkrētam mezglam varēs saprast tikai konkrētais mezgls, jo lai arī pa vidu stapr sūtītāju un saņēmēju ir daudzi lietotāju mezgli, tomēr pārtvert un atšifrēt datus cjdns protokolā nav iespējams.

Kopumā autors gribētu teikt, ka ir daudz priekšrocību cjdns protokola izmantošanai un ir zināmi trūkumi, taču trūkumi ir atrisināmi un principā ir komsummā mazāk nozīmīgi par priekšrocībām, autoraprāt.

REZULTĀTI

Darba rezultāti ir atbildējuši uz jautājumiem, kurus autors formulēja sākot darba izstrādi kā problēmas, uz kurām jārod risinājums.

Pirmkārt, darba gaitā tika apzinātas un izpētītas tās iespējas izmantot sietveida topoloģijas tīklus, kuras praktiski tiek realizētas dažādiem mērķiem un dažādos mērrogos. Autors nonāca pie secinājuma, ka sietveida topoloģija tiek pilnībā, bet parasti daļēji integrēta uzņēmumu vai citu organizāciju tīklos ar mērķi paaugstināt bojājumpiecietību vai arī uzlabot veiktspēju.

Bezvadu pašorganizējošies sietveida topoloģijas tīkli ir ļoti efektīvs veids, kā ātri, lēti un pieejami visiem, izplatīt tīklu un pieslēgumu lielajam tīmeklim vietās, kur ir sagrauta infrastruktūra pēc kādas katastrofas. Taču šādi tīkli tiek izmantoti lokālos, vienas pilsētas, reģiona vai valsts mērrogos ar mērķi arī miermīlīgos apstākļos bez pēdējās jēdzes problēmas, lēti un ātri pieslēgt lielu skaitu cilvēku tīklam. Šādi tīkli ir pierādījuši efektivitāti, piemēram Spānijā – Guifi un Grieķijā – AWMN.

Autors ir nonācis arī pie pētījumu rezultāta, kas liecina par to, ka pasaulē, tuvākajā vēsturē ir bijuši, un daži turpina attīstīties, mēģināumi un centieni izveidot globālu pašorganizējošos sietveida tīklu, kurš būtu kā alternatīva pašeizējajam Internet tīklam, kurā šobrīt ir problēmas ar cenzūru, privātumu, brīvību.

No šādiem mēģinājumiem viens no dzīvākajiem un veiksmīgākajiem ir Hyperboria tīkls, kurš pašreizējos apstākļos strādā divos režīmos – pa virsu Internet tīklam un fiziskā veidā. Jau šobrīdējais Hyperboria tīkls spēj nodrošināt ievērojami labāku privātuma līmeni, kas ir detalizēti aprakstīts darbā, kā arī potenciāli varētu pārtapt par pilnvērtīgi viena režīma – fizikā režīma – bezvadu sietveida globālu tīklu ar visām izrietošajām sekām un īpašībām, kas arī detalizēti aprakstītas darbā.

Autoram arī izdevās veikt pieslēgšanos Hyperboria tīklam, cjdns rīkla kompilāciju un konfigurēšanu, lai sasniegtu šo mērķi kā arī izdevās notestēt personīgo Hyperboria tīklā izvietotu tīmekļa serveri un jau esošus tīmekļa serverus un mezglus.

Taču autors iepazinās arī ar tām problēmām, kas neļauj jau šodien šādam tīklam kļūt par globālu tīklu un aizvietot klasisko Internet tīklu vismaz tādā veidā kāds tas ir šobrīd.

Kopumā darba mērķi ir sasniegti. Autora skats par doto problēmu ir ievērojami pilnveidojies un zināšanas par šobrīdējo un perspektīvo sietveida topoloģijas tīklu lomu pasaules komunikāciju tehnoloģiju jomā ir ievērojami pilnveidotas.

NOBEIGUMS

Darba izvirzītie mērķi ir pilnībā sasniegti un problēma atrisināta.

Sietveida topoloģijas pielietojums tīklu izveidē ir ļoti daudzveidīgs. Ir iespējams veidot tīkjlus pēc šādas topoloģijas gan korporatīvā vidē, piemēram, efektīvi organizēt darbinieku bezvadu pieslēgšanos uzņēmuma tīklam, gan arī paaugstinot bojājumpiecietību – jo decentralizēts tīkls vai kāds atsevišķs tīkla līmenis, kas izveidots pēc sietveida topoloģijas principiem ir ļoti grūti iznīcināms, jo katra iekārta ir savienota ar citām daudzos veidos.

Daudz plašākas perspektīvas sietveida topoloģijas izmantošanā ir lokālu pilsētu vai reģionu merroga tīklos un globālos sietveida tīklos.

Pašorganizējošies bezvadu sietveida tīkli ir tie tīkli, kurus var ērti, lēti un ātri organizēt lokālos mērrogos kādā krīzes situācijā, jo ar tīkla izplatību nodarbojas tīkla dalībnieki, un visi, kas pieslēdzas šim tīklam, paši to arī izplata tālāk. Šādi tīkli tiek izmantoti ne tikai krīzes situācijās, bet arī, lai pavisam parastos apstākļos vienkārši nodrošināt pieslēgumu tīmeklim dažādās vietās pasaulē, kur ar klasisko pieslēgumu, ko sniedz kāds interneta pakalpojumu sniedzējs, ir problēmas.

Uz darba galveno jautājumu – vai sietveida topoloģija varētu klūt par globāla tīkla pamata topoloģiju – ir iegūt pozitīva atbilde. Jo vairāk – ir mēģinājumi un centieni strādāt šajā virzienā, taču sabiedrība sastopas ar vairākām problēmām, kuras vispirms nepieciešams atrisināt, starp tām decentralizēta DNS radīšana, savienojumu minimālās kvalitātes garantēšana, savienojumi starp attālinātām tīklu saliņām un citas.

Izpētītais Hyperboria tīkls ir daudzsološs un perspektīvs, tas strādā un tiek attīstīts jau vairāku gadu garumā un pasaulē tam ir liels skaits atbalstītāju.

Nākotnē un turpmākajos pētījumos šajā sakarā būtu vēlams un iespējams veidot jau praktiskas koncepcijas kā risināt problēmas ar attālinātu saliņu savienošanu fizikā līmenī, DNS decentralizāciju, minimālās kvalitātes savienojumiem nodrošināšanu.

IZMANTOTĀ LITERATŪRA UN AVOTI

1. *Ячеистая топология.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/Ячеистая_топология
2. **Киселев М**. *Экспресс электроника. Ячеистые сети.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://citforum.ru/nets/wireless/mesh/
3. *Wi-Fi Mesh сети для самых маленьких* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/196562/
4. *IEEE 802.11s Wi-Fi Mesh для самых маленьких часть первая.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/199508/
5. *B.A.T.M.A.N.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/B.A.T.M.A.N.
6. *OLSR.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/OLSR
7. *Cjdns.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/Cjdns
8. *Nxt.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/Nxt
9. **Илембитов И**. *Как построить свою Mesh-сеть.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://xakep.ru/2014/09/05/mesh-networks/
10. **Изместьева Е**. *Мастерская по Mesh-сетям: что это такое и кому они нужны*. [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://te-st.ru/2013/09/06/mesh-networks-workshop-2/
11. *Анонимные сети.*[tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/Анонимные_сети
12. *Одноранговая сеть*. [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/Одноранговая_сеть
13. *Самоорганизующиеся сети.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://icfond.ru/it-/item/самоорганизующиеся-сети
14. *I2P.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/I2P
15. *I2P – Проект Невидимый Интернет.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/97827/
16. *Netsukuku.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://ru.wikipedia.org/wiki/Netsukuku

17. *Netsukuku – свой собственный интернет*. [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/86702/
18. *Hyperboria: Интернет 2.0.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/181862/
19. *Hyperboria: Как все устроено* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/182652/
20. *Hyperboria: Маршрутизация.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/183606/
21. *Интервью с Caleb James DeLisle, создателем cjdns*. [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/196646/
22. *Hyperboria.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://hype.rusblock.com/
23. *Cjdns.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://github.com/cjdelisle/cjdns/blob/master/README_RU.md
24. *Как подключиться к Hyperboria.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: http://habrahabr.ru/post/192252/
25. **RIPE NCC, Ripe Network Coordination Centre.** *IPv6 Address Types.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://www.ripe.net/manage-ips-and-asns/ipv6/ipv6-address-types/ipv6-address-types
26. *Known Hyperboria sites.* [tiešsaiste] – [atsauce 23.05.2015.]. Pieejams: https://wiki.projectmeshnet.org/Known_Hyperboria_sites

Bakalaura darbs „Sietveida topoloģijas tīklu iespēju pētīšana un analīze” izstrādāts LU Datorikas fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: _____ Oskars Zandersons

Rekomendēju/nerekomendēju darbu aizstāvēšanai

Vadītājs: lektora p.i. Dr.sc.comp. Leo Trukšāns _____ __.__.2015.

Recenzents: profesors Dr.sc.comp. Jānis Bičevskis

Darbs iesniegts Datorikas fakultātē 01.06.2015.

Dekāna pilnvarotā persona: vecākā metodiķe Ārija Sproģe _____

Darbs aizstāvēts bakalaura gala pārbaudījuma komisijas sēdē

__.__.2015. prot. Nr. ___.

Komisijas sekretāre: _____