PËRDORIMI I RRJETAVE MOBILE AD HOC WIRELESS NË KOMUNIKIMET NAVALE TË EMERGJENCËS, MUNDËSITË E APLIKIMIT NË SHQIPËRI

Esmeralda Hoxha

Dorëzuar
Universitetit Europian të Tiranës
Shkollës Doktorale

Në përmbushje të detyrimeve të programit të Doktoratës në
(Shkenca Ekonomike), me profil (Menaxhimi I Sistemeve Të Informacionit),
për marrjen e gradës shkencore "Doktor"

Udhëheqës shkencor: Mimoza Durrësi, Phd

Numri i fjalëve: 52,700

Tiranë, 2015

DEKLARATA E AUTORËSISË

Nën përgjegjësinë time personale, deklaroj se ky studim është punim origjinal dhe nuk përmban plagjaturë. Punimi është shkruar prej meje, nuk është prezantuar asnjëherë para një institucioni tjetër për vlerësim dhe nuk është botuar anjëherë. Punimi nuk përmban material të shkruar nga ndonjë person tjetër përveç rasteve të cituara dhe të referuara.

ABSTRAKTI

Niveli i lartë i sigurisë është një shqetësim i vazhdueshëm dhe në rritje. Aktiviteti detar i qëndrueshëm është vital për rritjen e sigurisë dhe ekonomisë botërore.

Ne jetojmë në kohën e Wireless, ku rritja e fuqisë së komunikimit dhe avancimi në teknologjinë e rrjetizimit wireless ofrojnë mundësi për aplikime të reja në komunikimet mjet-me-mjet. Komunikime efektive ndërmjet mjeteve janë rritur duke përdorur protokolle efektive të rutimit që marrin në konsiderate specifikimin e rrugëve nëpër të cilat kalojnë këto mjete si dhe të dhëna të detajuara për çdo mjet. Aplikacionet e reja të komunikimit mobile kërkojnë përmirësimin e cilësisë dhe të besueshmërisë të protokolleve dhe komunikimit ndërmjet mjeteve.

Rrjetat ad-hoc janë rrjeta spontane, të krijuara nga nyje spontane në mjedise me ose pa mbulim të rrjetit të zakonshëm celular. Në këtë përkufizim përshtaten dhe grupimet e anijeve në porte ose pranë tyre. Për këtë arsye në këtë punim komunikimi mes anijeve do të modelohet si komunikim mes nyjeve të rrjetit ad-hoc.

Duke u nisur nga rëndësia dhe roli që këto protokolle rutimi luajnë në komunikimin efektiv point-to-point, ky studim fokusohet në ndërtimin e një protokolli rutimi, të titulluar protokolli InterNavComm, në rrjetet ad hoc wirelees i cili merr në konsideratë të gjitha detajet specifike të komunikimit mes anijeve për një komunikim të shpejtë dhe efiçent.

Ideja kryesore në protokollin InterNavComm është krijimi i një infrastrukture virtuale hierarkike të përbërë nga qeliza me dimensione të caktuara(300-400m) dhe për çdo qelizë zgjidhet një anije që të shërbejë si qendër komunikimi për anijet e tjera në atë zonë. Kjo do të jetë baza e strukturës hierarkike të rrjetit ad-hoc të krijuar për anijet.

Pra ajo që ne do të realizojmë është një shërbim rutimi të kualifikuar në rrjetet sensor dhe ad-hoc wireless, menaxhim të fuqisë, vetë organizim, shpërndarje, mbulim dhe lokalizim. Kontributi ynë do të jetë rritja e efektivitetit, disponibilitetit dhe sigurisë në protokollet ad-hoc inter-navale.

Duke patur parasysh këtu që si në çdo portë edhe në portet shqiptare, gjithashtu edhe në portin e Vlorës të cilin e kemi marrë si rast studimi, ngrihet nevoja e aplikimeve të reja dhe më të sigurta, protokolli ynë InterNavComm, i cili është një protokoll që siguron komunikim të vazhdueshëm dhe të sigurtë ndërmjet anijeve edhe në rastet e mungesës së infrastrukturës, do të ndihmonte në plotësimin e mangësive ekzistuese sidomos në zonat me mungesë mbulimi valor.

Fjalë kyçe: Ad-hoc, Protokoll, Komunikim, Rrjet, Wireless, InterNavComm

ABSTRACT

High level of security is a continuing and growing concern. Sustainable maritime activity is vital for increased security and global economy.

We live in the age of wireless, where the growth of the power of communication and advancement in wireless networking technologies offer opportunities for new applications in vehicle-to-vehicle communications. Effective communications between vehicles increased by using effective routing protocols that take into account the specification of routes through which pass these vehicles and as well as detailed information for each vehicle. The new applications of mobile communications require the quality and reliability improvement of protocols and communications between vehicles.

Ad-hoc networks are spontaneous networks generated from spontaneous nodes on aereas with or without coverage of the ordinary mobiles network. In this definition fit even the groups of ships in their ports or nearby. For this reason in this paper the communication between vehicles will be designed as communication between nodes of ad-hoc network.

Considering the importance and the role that those routing protocols play in effective point-to-point communication, this study focuses on the construction of a routing protocol, entitled InterNavComm protocol, in ad hoc wirelees networks, that takes into account all

the specific details of the communication between the vehicles to a fast and efficient communication.

The main idea to InterNavComm protocol is to create a hierarchical virtual infrastructure composed of cells with specific dimensions (300 - 400m) and for each cell is elected a boat to serve as a communication hub for other ships to the area. This will be the basis of the hierarchical structure of the ad-hoc network created for ships.

So what we will implement is a qualifying routing service in sensor and ad-hoc wireless networks, power management, self organization, distribution, coverage and localization. Our contribution will be the increase of efficiency, availability and security at ad hoc inter-naval protocols.

Considering here as in every Albanian ports, as well as in the port of Vlora which we have taken as a case study, there is a necessity for new and safer applications, our InterNavComm protocol, which is a protocol that provides continuous and safely communication between ships even in the absence of infrastructure, will help to complement the existing deficiencies, especially in areas with a lack of wireless coverage.

Keywords: Ad-hoc Protocol, Communication, Network, Wireless, InterNavComm

DEDIKIMI

Familjes dhe Nënës Time

FALENDERIME

Me shumë mirënjohje do të falënderoja në radhë të parë udhëheqësen time të diplomës Znj. Mimoza Durrësi e cila me shumë profesionalizëm më ka orientuar dhe inkurajuar në këtë punim shkencor të rëndësishëm.

Një falënderim i veçantë është për bashkëshortin dhe prindrit e mi dhe sidomos për nënën time, të cilët më kanë ofruar mbështetje morale dhe qetësi gjatë kohës së studimit tim doktoral.

Dëshiroj të shpreh mirënjohje të veçantë ndaj mikut dhe kolegut Skënder Koltraka i cili ka dhënë kontributin i tij në arritjen me sukses të punimit tim.

Falënderoj gjithashtu edhe Universitetin Europian të Tiranës për mundësinë e dhënë.

PËRMBAJTJA E LËNDËS

LISTA E TABELAVE OSE DIAGRAMEVE

LISTA E FIGURAVE

KAPITULLI III

KAPITULLI IV

LISTA E SHKURTIMEVE DHE E FJALORIT

ISPS	International Ship and Port Security Code
IMO	International Maritime Organization
SOLAS 1974 (amended)	International Convention for the Safety of Life at Sea.
IMDG	International Maritime Dangerous Goods Code
LAN	Local Area Networks
WAN	Wide Area Networks
MANET	Mobile Ad hoc Network
AODV	Ad hoc On-demand Distance Vector
PDA	Personal Digital Assistant
NPDU	Network Layer Message discarded
RIP	Routing Information Protocol
IVC	Inter Vehicle Communication
LCS	Littoral Combat Ship
GS-802-11	"General Schedule"-Engineering Technical Series
CSP	Communication Service Provider
QoS	Quality of Service
SOA	Service-Oriented Architecture
SOLAS	International Convention for the Safety of Life At Sea 1974, as amended (references are usually to Chapter V of the Annex to that Convention – The Safety of Navigation).
DRS	Sensore Radar Digital

NMEA	National Marine Electronics Association energy efficient routing protocols
ICMP	Internet Control Message Protocol
DSDV	Destination-Sequenced Distance Vector
DSP	Digital Signal Processor
DSR	Dynamic Source Routing
GPSR	Greedy Perimeter Stateless Routing
GPS	Global Positioning System
FDMA	Frequency Division Multiple Access
IF	Intermediate Frequency
ISI	InterSymbol Interference
IEEE	Institute of Electrical and Electronics Engineers
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MBCR	Minimum Battery Cost Routing
MST	Minimum Spanning Tree
MTPR	Minimum Total Transmission Power Routing

HYRJE

Bazim teorik

Në përputhje me standartet e trafikut detar ndërkombëtar dhe në zbatim të të gjitha standarteve të përcaktuara në Konventën Ndërkombëtare Detare, në të cilën merr pjesë edhe Republika e Shqipërisë, çdo port (përfshirë këtu edhe portet në Shqipëri, portin e Durrësit dhe të Vlorës, porte këto të hapura për trafikun ndërkombëtar detar) është përgjegjës për të përmbushur kushtet dhe standartet e nevojshme për funksionim normal. Ndër këto standarte mund të përmendim: GS-802-11, ISPS, IMO, SOLAS 1974, IMDG,....

Niveli i lartë i sigurisë është një shqetësim i vazhdueshëm dhe në rritje. Aktiviteti detar i qëndrueshëm është vital për rritjen e sigurisë dhe ekonomisë botërore. Përparimi i shpejtë teknologjik në komunikimin e bazuar navigacional dhe hapësinor, kombinuar me karakteristikat rregullatore në rritje, si dhe presioni për të ulur sa më shumë rreziqet dhe koston përfaqësojnë mundësi të reja.

Ne jetojmë në kohën e Wireless[1], ku rritja e fuqisë së komunikimit dhe avancimi në teknologjinë e rrjetizimit wireless ofrojnë mundësi për aplikime të reja në komunikimet mjet-me-mjet.

Komunikimi wireless është, në çdo aspekt, segmenti më i shpejtë në rritje i industrisë së komunikimit. Si i tillë, ai ka tërhequr vëmendjen e medias dhe imagjinatën e publikut. Sistemet celulare kanë përjetuar rritje eksponenciale gjatë dekadës së fundit dhe aktualisht sot ka më tepër se dy miliardë përdorues në mbarë botën. Në të vërtetë, telefonat celulare janë bërë një mjet kritik në biznes dhe një pjesë e jetës së përditshme në shumicën e vendeve të zhvilluara, ato kanë zëvendësuar me shpejtësi sistemet e vjetëruara wired[2] në shumë vende në zhvillim. Përveç kësaj, në hapësirat lokale rrjetet wireless aktualisht plotësojnë ose zëvendësojnë rrjetet wired në shumë shtëpi, biznese dhe kampuse.

Shumë aplikacione të reja, duke përfshirë edhe rrjetet sensor wireless, autostradat e automatizuara dhe fabrikat, shtëpitë dhe pajisje e zgjuara dhe telemjekësinë e largët, po dalin nga idetë kërkimore në sisteme konkrete (T. Seymour, A. Shaheen, 2011).

[1] pa tel
[2] me tel

Duke u bazuar në karakteristikat e komunikimit wireless mobile, mund të themi se shërbimet e navigimit në rastet e emergjencës janë një aplikimi i rëndësishëm i rrjeteve sensor dhe ad-hoc wireless për shpëtimin dhe sigurimin e jetës së njerëzve.

Komunikime efektive ndërmjet mjeteve janë rritur duke përdorur protokolle efektive të rutimit që marrin në konsiderate specifikimin e rrugëve nëpër të cilat kalojnë këto mjete si dhe të dhëna të detajuara për çdo mjet. Aplikacionet e reja të komunikimit mobile kërkojnë përmirësimin e cilësisë dhe të besueshmërisë të protokolleve dhe komunikimit ndërmjet mjeteve.

Prandaj në këtë punim kemi menduar të prezantojmë një algoritëm rutimi, i cili merr në konsideratë problemet që lidhen me thithjen dhe shpërndarjen e mesazheve me anën e sinjaleve wireless, praninë e zonave 'gri', hazardet, në të cilat përjetohen pritje të rëndësishme, të ndryshueshme dhe të paqëndrueshme me kalimin e kohës dhe deri në rrezikun e dështimit të transmetimit.

Ky algoritëm rutimi bazohet në një guidë të sigurtë për njerëzit për të realizuar një dalje të shpejtë nga zona e rrezikut.

Historia e komunikimit Wireless. Vizioni i tij

Në këtë punim shkencor është shumë e rëndësishme të mësojmë rreth komunikimit wireless për të qënë më të qartë mbi bazimin teorik të kësaj teme.

Rrjeti i parë wireless është zhvilluar në epokën para-industriale. Këto sisteme transmetonin informacion përtej horizontit (për t'u zgjeruar më vonë nga teleskopët) duke përdorur sinjale tymi, pishtar sinjalizues, pasqyra pulsuese, fishekzjarre sinjal,etj.... Një grup i përpunuar i kombinimeve sinjal u zhvillua për të përcjellë mesazhe komplekse me këto sinjale rudimentare. Stacionet vëzhguese ishin ndërtuar mbi kodra dhe përgjatë rrugëve për të transmetuar këto mesazhe në distanca të mëdha.

> Këto rrjete të hershme të komunikimit u zëvendësuan në fillim nga rrjeti telegrafik (shpikur nga Samuel Morse në 1838), dhe më vonë nga telefoni. Në vitin 1895, disa dekada më pas u shpik telefoni, Marconi demonstroi transmetimin e parë në radio nga Isle of Wight në një rimorkiator 18 milje larg, dhe radio- komunikimi lindi. Rrjeti i

parë i bazuar në radio paketa, ALOHANET, u zhvillua në Universitetin e Hawaii në vitin 1971. Ky rrjet aktivizoi faqet kompjuterike me shtatë kampuse shtrirë mbi katër ishuj për të komunikuar me një kompjuter qëndror në Oahu nëpërmjet transmetimit të radios. Arkitektura e rrjetit përdori një topologji yll me kompjuter qëndror në hub_in e vet. Ushtria amerikane ishte jashtëzakonisht e interesuar në kombinimin e të dhënave të paketës dhe radio transmetimit të qenësishme për ALOHANET. Gjatë viteve 1970 dhe fillim të viteve 1980-Defense Advanced Research Projects Agency (DARPA) investoi burime të konsiderueshme për të zhvilluar rrjete duke përdorur paketat radio për komunikime taktike në fushën e betejës. Rrjetet e radio-packet gjetën gjithashtu aplikim komercial në mbështetje të shërbimeve pa tel në zona të gjerë . Këto shërbime, prezantuar më parë në fillim të viteve 1990, mundësuan access të të dhënave wireless(duke përfshirë email, transferim file, dhe shfletues web) në shpejtësi mjaft të ulëta, në rendin e 20 Kbps. Por këto shërbime kryesisht u zhdukën në vitet 1990, duke u zëvendësuar nga kapaciteti i të dhënave wireless të telefonisë celulare dhe të rrjeteve private LAN(Local Area Networks). Në vitin 1985 Komisioni Federal i Komunikimeve (FCC) mundësoi zhvillimin komercial të wireless LAN duke autorizuar përdorimin publik të brezave të frekuencave Industrial, shkencor, dhe Mjekësor(ISM) për produkte wireless LAN. Grupi ISM ishte shumë tërheqëse për shitësit e wireless LAN pasi atyre nuk u nevojitej të merrnin një licencë FCC për të vepruar në këtë brez. Për më tepër, interferenca nga përdoruesit primare brenda këtij brezi frekuencash ishte mjaft i lartë. Si rezultat i këtyre LAN fillestarë wireless kishte performancë shumë të dobët në drejtim të normave të të dhënave dhe mbulimit(T. Seymour, A. Shaheen, 2011).

Brezi i tanishëm i wireless LAN, bazohet mbi standartet e familjes të IEEE 802,11. Pavarësisht dallimeve të mëdha të normave të të dhënave, wireless LAN po bëhet metodë e preferuar e aksesit në Internet në shumë shtëpi, zyra dhe mjedise kampusi për shkak të lehtësisë/komoditetit dhe mos varësisë së tyre nga telat. Megjithatë, shumica e wireless LAN mbështetin aplikacione të tilla si e-mail dhe web browsing që

nuk janë Bandwidth[3]-intensiv. Deri tani aplikimi më i suksesshëm i rrjeteve wireless ka qenë sistemi telefonik celular. (T. Seymour, A. Shaheen, 2011).

Vizioni i komunikimit wireless: është të mbështesë shkëmbimin e informacionit midis njerëzve apo pajisjeve edhe në dekadat e ardhshme të komunikimit, dhe shumica e tij tashmë ekziston në disa forma. Ky vizion do të lejojë komunikimin multimedial kudo në botë duke përdorur një pajisje të vogël handheld[4] apo laptop. Rrjetet wireless do të lidhin palmtop, laptop, kompjutera desktop kudo brenda një zyre godine apo kampusi. Në shtëpi këto rrjete mundësojnë një klasë të re të pajisjeve inteligjente elektronike që mund të ndërveprojnë me njëri-tjetrin dhe me internet përveç sigurimit të lidhjes ndërmjet kompjuterave, telefonave, dhe sistemeve të sigurisë/monitorimit. Argëtimi Wireless ka përfshirë shtëpinë dhe çdo vend ku njerëzit mblidhen së bashku. Video telekonferencat zhvillohen edhe ndërmjet ndërtesave që janë blloqe ose kontinente larg, dhe këto konferenca mund të përfshijnë udhëtarët, apo dhe shitësin të cilit mund ti ketë humbur avioni për shitjet CEO në Karaibe. Wireless video do të mundësojë klasa mësimore në largësi, objektet të trajnimit në largësi, dhe lidhjet në largësi të spitaleve kudo në botë. Sensorët wireless kanë një gamë të madhe të të dy aplikimeve, komerciale dhe ushtarake(T. Seymour, A. Shaheen, 2011).

Aplikimet komerciale përfshijnë monitorimin e rreziqeve nga zjarri, shfaqjet e mbeturinave të rrezikshme, stresit dhe tendosjet në ndërtesa dhe ura, të lëvizjes së dioksidit të karbonit, përhapjen e kimikateve dhe faqeve mbi katastrofat e gazrave. Aplikimet ushtarake përfshijnë identifikimin dhe ndjekjen e objektivave të armikut, zbulimin e sulmeve kimike dhe biologjike, mbështetjen e automjeteve pa pilot robotik, dhe kundër-terrorizmit. Së fundi, rrjetet wireless mundësojnë sistemet e shpërndarë të kontrollit, me pajisje të largëta, sensorë, dhe aktivizuesit të lidhura së bashku me anë të kanaleve të komunikimit wireless. Rrjete të tilla mundësojnë autostrada te automatizuar, robots celulare, si dhe automatizimin industrial lehtësisht të rikonfigurueshëm(T. Seymour, A. Shaheen, 2011).

[3] Gjerësi-brezi
[4] Pajisje dore/palmar

1G

Rrjeti celular tregtare, i automatizuar, i parë (gjenerata 1G) u prezantua në Japoni nga NTT në vitin 1979, fillimisht në zonën metropolitane të Tokios. Rrjeti i parë 1G lançua në SHBA ishte Ameritech Chicago-based në vitin 1983 duke përdorur telefonin celular Motorola DynaTAC. Sistemi i parë analog celular vendoset në Çikago në vitin 1983 ishte thelluar tashmë nga 1984.

2G

Gjenerata e dytë e sistemeve celulare, të vendosur për herë të parë në fillim të viteve 1990, ishin bazuar në komunikimet dixhitale. Ndërsa sistemet e brezit të dytë celular fillimisht ofruan kryesisht shërbime zanore, këto sisteme evoluan gradualisht për të mbështetur shërbimet e të dhënave të tilla si email, akses në Internet, dhe mesazhe të shkurtër.

3G

International Mobile Telecommunications-2000 (IMT - 2000), i njohur më mirë si 3G apo Gjenerata 3G është një brez i standardeve për telefonat mobil dhe shërbimeve të telekomunikacionit celular duke përmbushur specifikimet nga Unioni Ndërkombëtar i Telekomunikacionit. Shërbimet e aplikimit përfshijnë telefoninë, akses në internet mobile, thirrje-video dhe TV celular, të gjitha në një mjedis të lëvizshëm. Krahasuar me standartet e vjetër 2G dhe 2.5G , një sistem 3G duhet të sigurojë normat e të dhënave më të paktën deri 200 kbit/s sipas specifikimit IMT-2000. 3G, gjithashtu siguron akses broadband mobile deri në disa Mbit/s në kompjutera laptop dhe Smartphone.

Transmetimi i lartë i rangut të të dhënave:

- 144 kbps me mbulimin total për përdorim mobil
- 384 kbps me mbulim të mesëm për përdorim të këmbësorëve
- 2 Mbps me sipërfaqe të reduktuar mbulimi për përdorim të palëvizshëm

4G

LTE i avancuar (afatgjatë-evolucioni i avancuar) është një kandidat për standardin IMT-i avancuar, paraqitur zyrtarisht nga organizata 3GPP për të ITU-T(International

Telecommunications Union) në vjeshtë të vitit 2009, dhe pritet që do të dalë në vitin 2012. Objektivi i 3GPP LTE i avancuar është për të arritur dhe tejkalojnë [14] kërkesat L ITU. Kjo nuk është një teknologji e re, por më tepër një përmirësim në rrjet LTE ekzistues ITU_r.

Në rrjetet Tipike wireless: Bazuar në infrastrukturë p.sh., GSM, UMTS, ...

- Stacionet bazë lidhen në një rrjet me mbështetje me tel.
- Subjektet Mobile komunikojnë me valë ndërmjet këtyre stacioneve bazë
- Trafiku ndërmjet subjekteve të ndryshëm celular kalon prej stacioneve bazë dhe shtyllat mbështetëse me tel
- Lëvizshmëria mbështetet prej kalimit nga një stacion bazë në tjetrin
- Infrastruktura mbështetëse e nevojshme për detyrat administrative

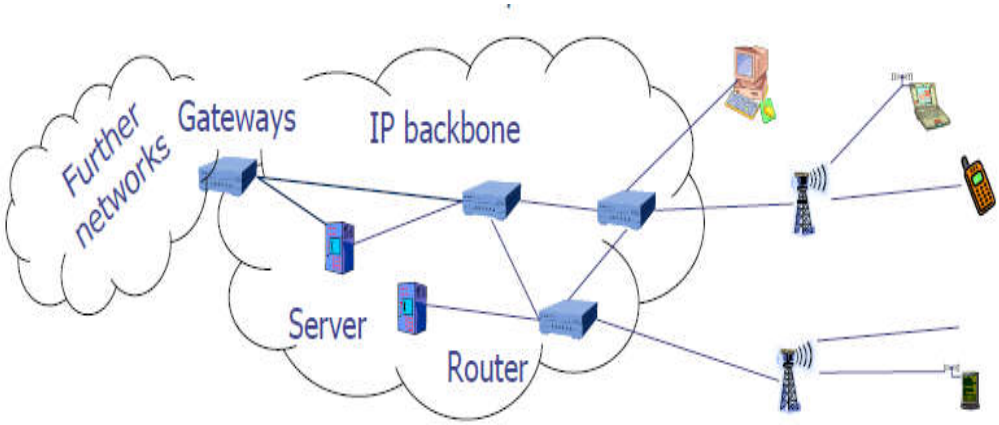


Figura 1. Infrastukturë për rrjetet wireless.

Limitimet:

Po nëse …

- nuk ka Infrastrukturë në dispozicion? -P.sh., Në zonat e fatkeqësisë
- ndoshta është shumë i shtrenjtë / i papërshtatshëm për tu ngritur? –P.sh., Në largësi, e site me konstruksion të madh.
- nuk ka kohë për ta vendosur atë? -P.sh., Në operacionet ushtarake

Problemet/sfidat për rrjetet ad hoc pa një infrastrukturë qëndrore:

Gjërat bëhen shumë më të vështira nëse problemet janë për shkak të:

- Mungesës së një njësie qëndror për mundësi organizimi
- Rang i limituar në komunikimet pa tel
- Mobiliteti i pjesëmarrësve/ambjente shumë dinamike
- Subjektet operojnë me bateri

Aplikimet e mundshme për rrjetet pa infrastrukturë:

- Rimëkëmbje fatkeqësish
- Komunikim makinë-me-makinë
- Rrjete ushtarake: Tanke, ushtarë, ...
- Gjetja e vendparkimeve bosh në një qytet, pa kërkuar një server
- Kërkim dhe shpëtim në një ortek
- PAN(Personal Area Network) (shikim, syze, zbatime mjeksore....)

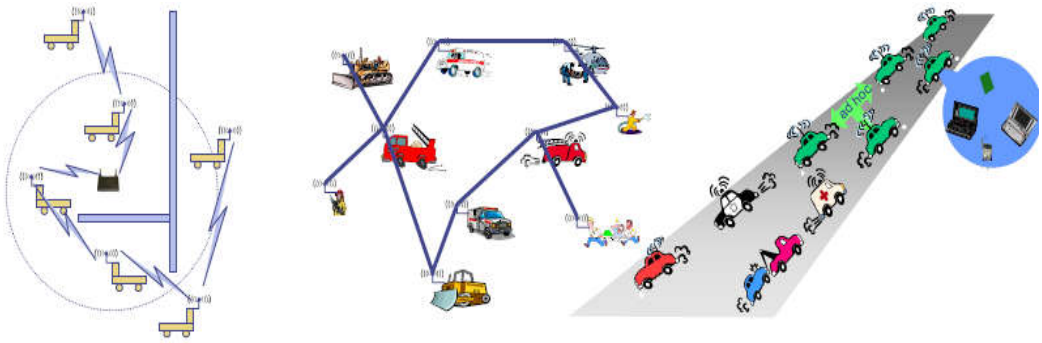


Figura 2. Aplikime të mundshme për rrjetet me infrastrukturë të lirë (H.Karl,Computer Networks Group)

Mobiliteti! Protokollet e përshtatshëm

- Në shumë (jo në të gjitha!) aplikacione të rrjetit Ad hoc, pjesëmarrësit lëvizin në:
  - rrjeta celular: thjesht dorëzoje në një tjetër stacion bazë
- Rrjetet mobile ad hoc (MANET):
  - Mobiliteti ndryshon marrëdhëniet në fqinjësi
  - Duhet të kompensohen për...

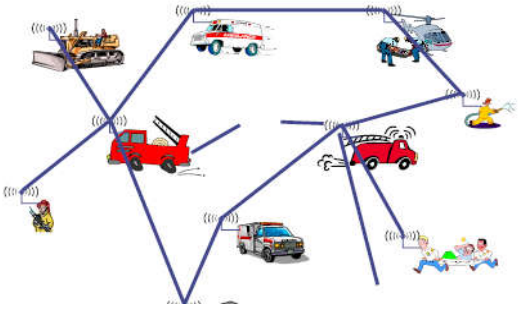


Figura. 3 Lëvizshmëria në një rrjet mobile ad hoc

- P.sh., rrugët në rrjet duhet të ndryshohen

- Të komplikuar nga shkallëzueshmëria
  - Numri i madh i nyjeve të tilla vështirë për t'i mbështetur

Gjatë këtij studimi mbi komunikimet në rrjetet ad hoc wireless duhet të kemi parasysh se proçesi i komunikimi ose i kalimit të mesazhit duhet të jetë projektuar për të ruajtur burimet e kufizuara energjetike të sensorëve.

Klasterimi[5] në rrjetet mobile ad hoc (MANETs) dhe rrjetet sensor wireless (WSNs) është një metodë e rëndësishme për të lehtësuar menaxhimin topologjik dhe rutimin[6] në rrjete të tilla. Pasi klasterat janë formuar/kryer, udhëheqësit klaster mund të përdoren për të formuar një shtyllë për qëllime rutimi dhe komunikimi efiçent. Një grup i klasterave mund të sigurojë strukturën themelore fizike për komunikim multicast për një modul komunikimi grup në nivelin më të lartë i cili në fakt mund të përdoret për tolerimin e gabimit dhe menaxhim kyç për qëllime të sigurisë. Sensorët klasterizohen, kështu që nëse sensorët komunikojnë informacionin vetëm në krerët cluster dhe pastaj krerët cluster e komunikojnë informacionin e grumbulluar në qendrën e përpunimit, mund të kursejnë energji.

Një rrjet sensor wireless (WSN) është një rrjet wireless/pa tel të shumë nyjeve sensore autonome të energjisë-ulët, kosto të ulët, dhe me madhësi të vogël që janë vetë-organizuese dhe përdorin sensorë bashkëpunues për të monitoruar kushtet e ndërlikuara fizike apo mjedisore, të tilla si lëvizja, temperatura, tingulli etj. Sensorë të tillë janë në përgjithësi të pajisur me aftësi për përpunimin e të dhënave dhe të komunikimit dhe janë vendosur në skenarë të brendshëm p.sh., shtëpi dhe zyre, ose skenarët në natyrë si mjediset natyrore, ushtarake dhe të ngulitur.

Këto nyje komunikojnë me njëri-tjetrin duke shkëmbyer të dhënat e grumbulluara apo informata të tjera me rëndësi jetike për të monitoruar një mjedis të veçantë.

Një rrjet sensor wireless është një rrjet prej shumë pajisjesh të vogla të energjisë-ulët, të quajtura nyje, të cilat janë të shpërndara në hapësirë me qëllim kryerjen e një detyre globale aplikim-orientuar. Këto nyje formojnë një rrjet duke komunikuar me njëri-tjetrin në mënyrë

[5] Grupimi
[6] Rrugëzimi/kursi

të drejtpërdrejtë ose nëpërmjet nyjeve te tjera. Një ose më shumë nyje midis tyre do të shërbejnë si tuba që janë të aftë për të komunikuar me përdoruesit ose direkt ose nëpërmjet rrjeteve ekzistuese Wired. Ku komponenti kryesor i rrjetit është sensori, i rëndësishëm për monitorimin e kushteve fizike të botës reale të tillë si tingulli, temperatura, lagështia, intensiteti, vibrimi, presioni, ndotja etj...

Është e rëndësishme në këtë punim të njihemi edhe me fushat e aplikimit të këtyre tipe rrjetash dhe shtrirjen që ato kanë:

- **Ushtri**
  - Zbulimi i ndërhyrjeve në bazë.
  - Zbulimi i lëvizjeve të njësive armike në tokë e në det.
  - Mbikqyrje në fushë- betejë.
  - Monitorimi forcave armiqësore
  - Monitorimi i forcave miqësore dhe pajisjeve
  - Targetimi
  - Vlerësimi dëmi në beteja
  - Zbulimin sulm biologjik, kimik dhe bërthamore
- **Situata Emergjence**
  - Menaxhimin e Katastrofave
  - Detektorë të zjarrit / ujit
  - Nivele kimike të rrezikshme dhe sensor zjarresh
- **Botën Fizike**
  - Monitorim mjedisor të ujit dhe dheut
  - Monitorime te zakonshme/përhershme
  - Vëzhgimi i sistemeve biologjik dhe artificial
- **Mjeksi dhe Shëndet**
  - Sensorë për matjen e fluksit të gjakut dhe shkallën respiratore
  - ECG(electrocardiogram)
  - Monitorimin në distancë të të dhënave fiziologjike
- **Automatizim dhe kontroll, të tillë si kontrolli robotikë**
- **Automatizimin Industrial**

- **Rrjetizimi në shtëpi e zyra**

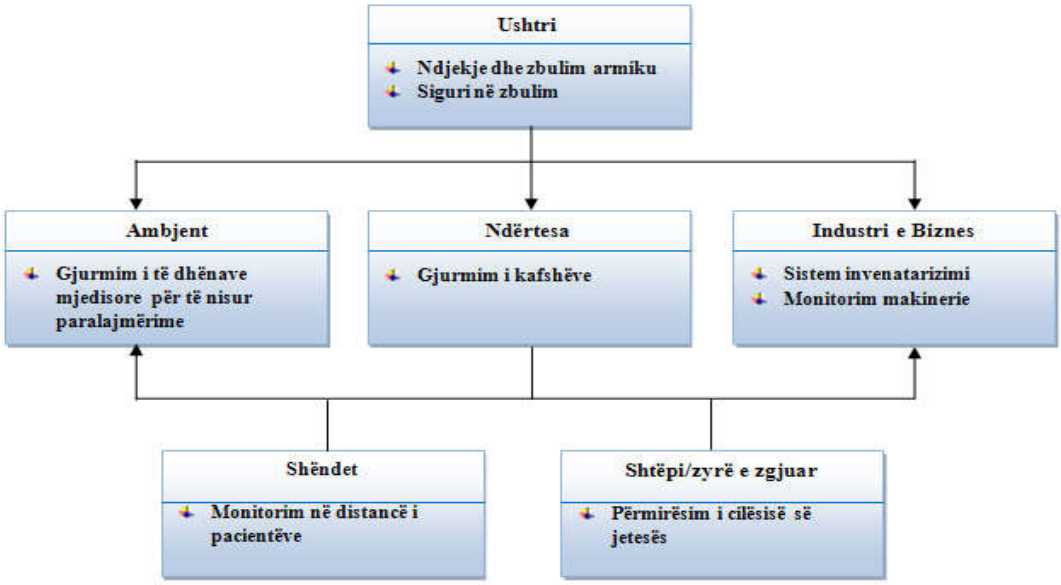


Diagrama 1. Zhvillimi i aplikimeve në rrjetet sensore i skematizuar

Objekt i studimit dhe Shtrimi i problemit

Që nga shfaqja e tyre më 1970_ën, rrjetet wireless janë bërë gjithmonë e më shumë popullore në industrinë informatike.

Në komunikimin anije-anije, komunikimi i lëvizshëm ad-hoc është i përshtatshëm pasi ai ofron pathet e komunikimit alternative për infrastrukturat e komunikimit pa nevojën e mbulimit nga stacionet bazë.

Sigurisht struktura hierarkike e një protokolli për komunikim, bën të mundur optimizimin e proçesit të rutimit. Protokolle të ndryshme rutimi janë zhvilluar për rrjetet ad-hoc wireless.

Sistemet taktike tradicionale të komunikimit konsistojnë në një numër nënsistemesh të ndara me ndërlidhje (interworking) të vogla ndërmjet tyre dhe me sensor të jashtëm.

Krahasuar me këto sisteme mund të theksoj se rrjeti ad-hoc wireless është një nga arkitekturat më të përshtatshme për rrjetet mobile.

Një rrjet mobile ad-hoc është një grup nyjesh të lëvizshme të cilat bashkarisht dhe spontanisht krijojnë një rrjet. Pra lëvizshmëria shkakton dhe ndryshimet e rrugës. Mund të themi se një rrjet mobil ad hoc (MANET), është një rrjet i përbërë nga rutera wireless të lëvizshëm MR(Mobile Roters) që komunikojnë me njëri-tjetrin pa kontroll të centralizuar.

Dinamika e rrjeteve pa tel ad hoc rrjedh si pasojë e lëvizshmërisë dhe e shkyçjes së hostit të lëvizshëm.

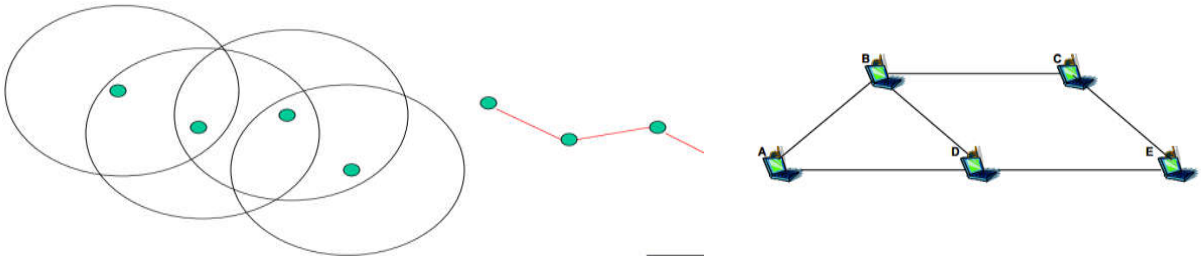


Figura 4. Strukturë e thjeshtë e një rrjeti mobile dhe rrugëzimi i krijuar nga mobiliteti

Siç mund të kemi cilësuar më lartë rrjetat ad-hoc janë rrjeta spontane, të krijuara nga nyje spontane në mjedise me ose pa mbulim të rrjetit të zakonshëm celular. Këtij përkufizimi i përshtaten dhe grupimet e anijeve në porte ose pranë tyre. Për këtë arsye në këtë punim komunikimi ndërmjet anijeve do të modelohet si komunikim ndërmjet nyjeve të rrjetit ad-hoc. Përdorimi i protokollit InterNavComm që merr në konsideratë të gjitha detajet specifike të komunikimit mes anijeve do të prezantojë një komunikim të shpejtë dhe efiçent.

Pra do ne të merremi me një shërbim rutimi të kualifikuar në rrjetet sensor dhe ad-hoc wireless, menaxhim të fuqisë, vetë organizim, shpërndarje, mbulim dhe lokalizim.

Ideja kryesore në protokollin InterNavComm është krijimi i një infrastrukture virtuale hierarkike të përbërë nga qeliza me dimensione të caktuara(300-400m) dhe për çdo qelizë zgjidhet një anije që do të shërbejë si qendër komunikimi për anijet e tjera në atë zonë. Kjo do të jetë baza e strukturës hierarkike të rrjetit ad-hoc të krijuar për anijet.

Ne i konsiderojmë anijet si nyje të një rrjeti ad-hoc, të ndarë në qeliza virtuale që formojnë infrastrukturën virtuale specifike për këtë protokoll. Nyjet në një sipërfaqe të madhe, që

mund të përfaqësojë sipërfaqen e zonës rreth portit, janë organizuar në tre nivele të hierarkisë.

Në nivelin e parë janë përfshirë të gjitha nyjet në një qelizë. Këto nyje komunikojnë me njëra-tjetrën dhe ato gjithashtu mund të komunikojnë me nyjet e qelizave respektive fqinjë, të cilat janë në një fushë ose linjë komunikimi.

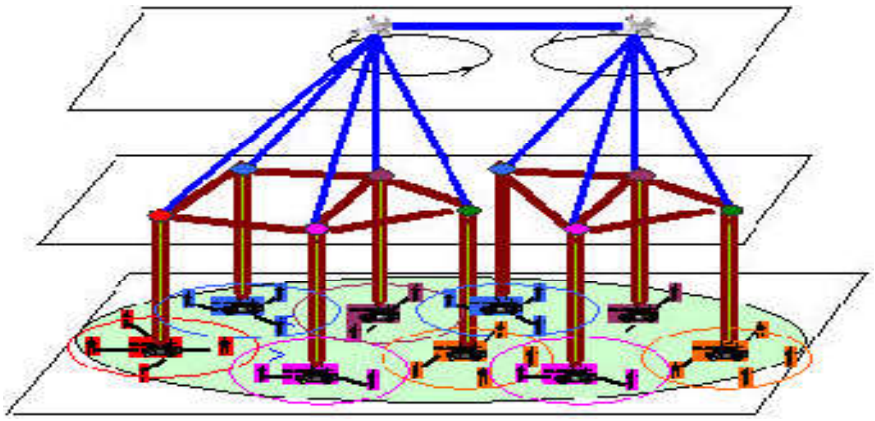


Figura 5. Komunikimi hierarkik i nyjeve në një rrjet ad- hoc

Niveli i dytë hierarkik është i përfaqësuar nga ato që i quajme 'Qendër Qelizat'(CC-Cell Center), të cilat janë një grup i vogël nyjesh të vendosura afër qendrës gjeografike të çdo qeliz. CC mund të komunikojë me antarët e qelizave respektive ose antarët e qelizave fqinjë që janë në një linjë komunikimi me CC. Komunikimi ndërmjet nyjeve të një qelizë me atë të CC respektive përfaqëson komunikimin e nivelit te dytë të hierarkisë me nivelin e parë.

Komunikimi ndërmjet anëtarëve në nivel të dytë të hierarkisë përfaqësohet nga komunikimi midis CC_ve. Kjo është e mjaftueshme që ato të komunikojnë në mënyrë sekuenciale njëra pas tjetrës kështu që çdo CC mund të komunikojë me njërën nga CC_at fqinjë.

CC_at fqinjë sillen si pjesë e zinxhirit që lidh qendrën aktuale(korente) me gjithë gjatësinë e rrugës në tërësi.

Është e rëndësishme të theksohet se pozicioni i CC_ve optimizon(përmirëson) komunikimin brenda qelizës dhe me qelizat fqinjë, duke mundësuar që të ketë cilësi të ngjashme transmetimi thuajse me të gjithë antarët e qelizës.

Përveç kësaj, çdo CC mban pothuajse një cilësi simetrike në komunikimin me qendrat fqinjë(më të afërta), duke siguruar kështu një barazpeshë ose cilësi të ekuilibruar për të dy drejtimet e lëvizjes së informacionit.

Pra kërkesa e vetme për të qenë një CC është që të jetë në një linjë komunikimi me antarët Qelizë. Në këtë filozofi dhe këndvështrim do të vazhdoj të shtrihet studimi im.

Niveli i tretë hierarkik është NC(Network Centers) që mbajnë të update_uar informacionin e vendodhjes për të gjitha nyjet në rrjet duke siguruar informacionin për CC.

Protokolli InterNavComm do të ishte shumë konvenient në komunikimet navale të emergjencës. Supozohet se një mesazh emergjence duhet të transmetojë ose shpërndahet menjëherë dhe në numër minimal hopesh ky mesazh duhet të merret nga të gjitha nyjet. Në rastin e përmbytjes(flooding) do të kishim një mbingarkim të rrjetit duke rezultuar në humbje të sinjalit dhe vonesa në komunikim. Duke përdorur këtë infrastrukturë hierarkike virtuale, pra protokollin InterNavComm, ngarkesa e rrjetit bie ndjeshëm, bëhet broadcast vetëm te CC ose liderat qelizë dhe këta të fundit te çdo anije në veçanti.

Qëllimi i studimit

Qëllimi *është që shpërndarja ose dorëzimi i mesazheve apo emergjencave të navigimit të bëhet në kohën e duhur, duke përdorur sa më pak burime të rrjetit dhe në kohën më të shkurtër të mundshme.*

Shërbimet e navigimit në rastet e emergjencës mund të jenë një aplikim i rëndësishëm i rrjeteve sensor dhe ad-hoc wireless për shpëtimin dhe sigurimin e jetës së njerëzve.

Kjo temë fokusohet në mundësimin dhe optimizmin e komunikimit ndërmjet nyjeve të një rrjeti ad-hoc që modelon rrjetin e komunikimit ndërmjet anijeve në port ose zonat përreth.

Hipotezat e punimit dhe Pyetjet kërkimore të punimit

Hipoteza: *Rritja e efektivitetit, disponibilitetit dhe sigurisë në protokollet ad-hoc inter-navale është një domosdoshmëri. Protokolli i ri InterNavComm është një protokoll i ri që siguron komunikim të vazhdueshëm dhe të sigurtë ndërmjet anijeve edhe në rastet e mungesës së infrastrukurës.*

Në portet shqiptare ngrihet nevoja e krijimit të aplikimeve të reja dhe të besueshme. Implementimi i protokollit InterNavComm edhe në portin e Vlorës do të ndihmonte në plotësimin e mangësive ekzistuese sidomos në zona me mungesë mbulimi valor.

Pyetja kërkimore: *Duke u nisur nga qëllimi që duam të arrijmë: A është me të vërtetë efiçent përdorimi i protokollit* InterNavComm *të rutimit për rrjetat ad-hoc wireless në navigacion, në komunikimin pikë me pikë/ anije me anije?*

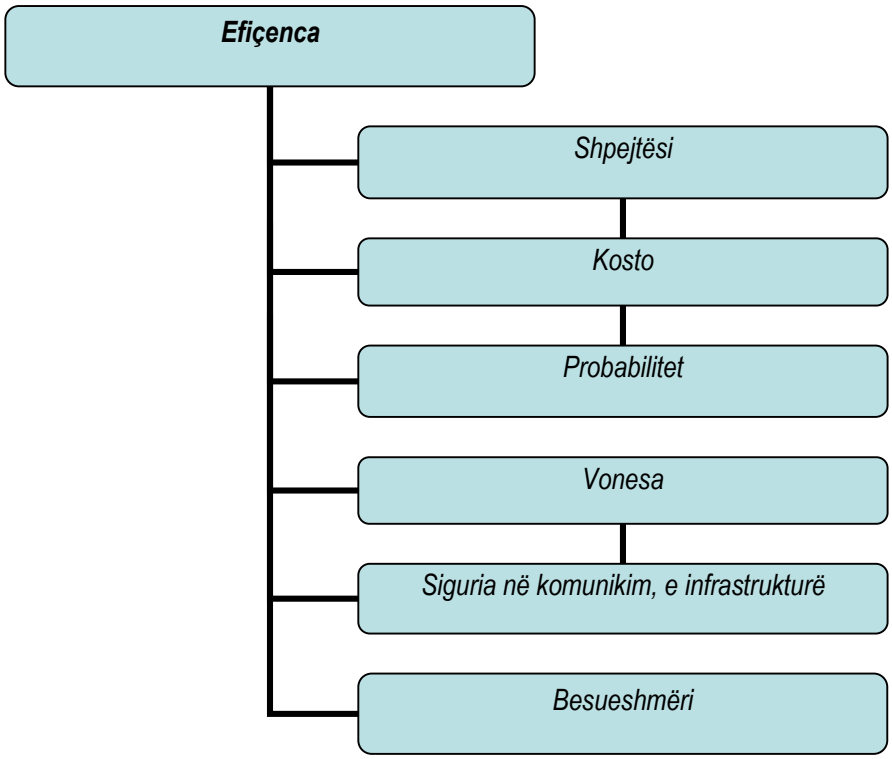


Diagrama 2. Zbërthimi i një procesi më të madh në procse më të vogla

Sigurisht duke copëtuar një proçes të madh në shumë të vegjël, lindin pyetjet e më poshtme:

- Si do të bëhet modelimi i rrjetit të kompjuterave në një rrjet wireless ad-hoc?
- Cili do të ishte modeli më i mirë i përafrimit?
- Cilët janë protokollet dhe strukturat ekzistues të komunikimit internaval në botë?
- Po në Shqipëri, veçanërisht në Vlorë?

- Cilat janë specifikat e dallimit të rrjetit të anijeve nga rrjeti i makinave në rastin e inter-vehicle communications,etj.
- Cilat do të ishin përdorimet e një protokolli të veçantë për komunikimet navale.
- A ka nevoje per protokolle te vecanta dhe pse?
- Cila është eksperienca e vendeve të huaja në këtë drejtim?
- A ekziston një përfitim financiar në përdorimin e këtij protokolli?
- A ekziston një përfitim qualitativ në përdorimin e këtij protokolli?
- Si do të përcaktohet vendodhja e çdo anije në çdo çast të kohës?
- Pse zgjedh simulatorin NS2?
- Në cilat kushte supozohet të realizohen simulimet?

Metodat dhe Metodologjia e Kërkimit

Të dyja metodat, analiza teorike dhe simulimi në kushte laboratorike duke përdorur simulatorin NS2, konfigurojnë avantazhin e këtij propozimi, si dhe krahasimi i protokollit tonë InterNavComm me protokolle të tjera ekzistues. Në analizë apo modelin teorik ne do të studiojmë çështje të ndryshme të sigurisë dhe zgjidhjet e tyre. Në modelin e simulimit ne do të vazhdojë me simulim duke u përpjekur të mësojmë mekanizmat të cilat do të na ndihmojnë për të zbatuar sigurinë në rrjetat Mobile ad hoc.

Si fillim kemi përdorur metodën e analizës teorike për të qënë më të qartë mbi bazimin teorik të kësaj teme, duke nisur të flasim që në hyrje mbi komunikimin wireless, vizionin dhe shtrirjen e tij, të mirat dhe vlerat që ky komunikim sjell por edhe mbi problemet dhe fushat e aplikimit. Në vazhdim në kapitullin e parë, tek Protokollet e Komunikimeve Ndër-Navale, shprehet qartë se përdorimi i rrjeteve sensor dhe ad-hoc wireless është i rëndësishëm për shpëtimin dhe sigurimin e mjeteve navigacionale dhe jo vetëm por edhe të jetës së njerëzve që ndodhen në to, si dhe evidentohen problemet që hasen gjatë komunikimeve ndër-navale dhe nevojën e tyre për protokolle të reja rutimi. Më pas bazimi teorik vazhdon me komunikimin Ad-hoc mobile, si një komunikim i sigurtë dhe efiçient, me llojet e

protokolleve ad-hoc wireless, një 'familje' në të cilën do të bëjë pjesë edhe protokolli ynë i rutimit, protokolli InterNavComm.

Metoda e simulimit dhe ajo e krahasimit midis 2 protokolleve do të përdoren më pas për të mbështetur ecurinë e këtij kërkimi dhe për të vërtetuar hipotezën e ngritur në këtë punim.

Siç mund të kuptohet, në themel të të gjithë studimit është transmetimi i mesazheve pra vazhdimësia e komunikimit.

Nyjet komunikojnë me njëra-tjetrën:

- Nyjet komunikojnë me "disa" nyje në një rrjet tjetër(p.sh Web server në Internet)
- Zakonisht kërkohen disa lidhje të rrjetit fiks.

Në një rrjet ad-hoc, topologjia e rrjetit ndryshon dinamikisht për shkak të lëvizjes së hosteve mobile. Këto lloj topologjish gjenerojnë paketa kontrolli mbi shtresën e aplikimit, që nëpërmjet tyre të arrijnë të kuptojnë informacionin mbi topologjinë e rrjetit. Kështu arrin që të rritet kontrolli i trafikut në të gjithë rrjetin.

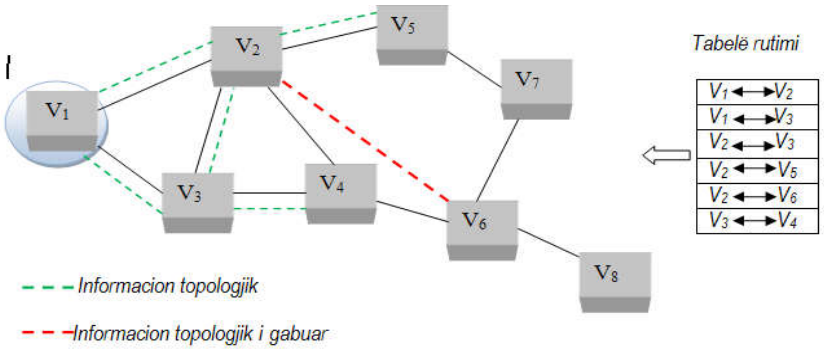


Figura 6. Topologjia e rrjetit ad-hoc

Për të vlerësuar performancën e protokollit marrim parasysh 2 metrika: **Vonesa (End-to-End) Pikë me pikë,** e matur ne ms. Kjo përdoret për shkëmbim informacioni ndërmjet burimeve dhe destinacioneve të ndryshme të marra rastësisht dhe që kanë distancë të ndryshme ndërmjet tyre. Sigurisht rezultatet varen nga ngarkesa e trafikut, shpeshtësia e mjeteve.

Ngarkim rutimi, i matur në bazë të numrit të mesazheve që transmetohen për çdo burim komunikimi në destinacion. Për të patur ide më të qarta, protokollin tonë të rutimit e

krahasojmë me protokolle të tjera rutimi, p.sh me një protokoll të njohur të përdorur në rastin kur kemi vërshime ose e njohur ndryshe “përmbytje”/flooding.

Si simulator kemi përdorur simulatorin NS2, simulator diskret ngjarjeje që drejtohet/ tragetohet në hulumtim të rrjeteve. Ky simulator siguron mbështetje të konsiderueshme për simulim të TCP, rutimit, dhe protokolleve multicast mbi rrjetet me tel dhe pa tel (lokale dhe satelitore).

Për të dy protokollet, krahasohet numri total i mesazheve të shkëmbyera ose ngarkim rutimi për çdo burim-destinacion dhe nxjerrim si përfundim se cili prej protokolleve, protokolli i paraqitur prej nesh apo ai i marrë për krahasim, paraqet performancë më të lartë.

Rëndësia e Studimit, Mundësitë dhe Kufizimet.

Në këtë studim mbështetemi mbi protokollin GS- 802.11, një standart ky i njohur dhe miratuar për rrjetet lokal wireless, i cili:

- Vepron në një brez/band të palicencuar 2,4 GHz ISM (Industriale & Shkencore & Mjekësi) Band
- 802.11 MAC punon me shtresa të ndryshme fizike (infra të kuqe, si dhe spektër përhapjen)
- I ndërveprueshëm me standardet e tjera 802.x, p.sh. 802,3 (Ethernet), 802,5 (unazë Token)
- Normat e të dhënave 1 Mbps (i detyrueshëm), 2 Mbps (optional)
- Mbështet aplikacionet si në kohë reale dhe ato në kohë jo-reale

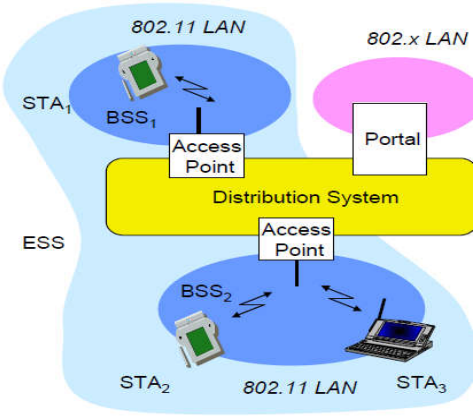


Figura 7. Standarti 802.11

- Ka karakteristika për menaxhimin e energjisë për të kursyer bateri 802.11 - Arkitektura e një rrjeti infrastrukturor
- Stacioni (STA): terminal me mekanizma aksesi wirelees dhe radio kontakt deri në pikën e aksesit.
- Basic Service Set (BSS)/Grup shërbimesh kryesore

  - Grup stacionesh duke përdorur të njëjtat frekuenca radio
  - Access Point
- Stacioni i integruar në LAN wirelees dhe sistemin e shpërndarjes
- Portal:urë (Wired) për rrjete të tjera
- Sistem shpërndarës
  - Rrjeti ndërlidhës për të formuar një rrjet logjik (EES: Extended Service Set) i bazuar në disa BSS

Me rëndësi është të përmendim dy faktorët kryesor të përdorur nga standarti GS-802 për vlerësimin e pozicioneve: Natyra e caktimit dhe Niveli i përgjegjësisë.

Natyra e caktimit: Ky faktor përfshin qëllimin dhe vështirësinë e projektit dhe aftësitë dhe njohuritë e nevojshme për të përfunduar detyrën.

Niveli i përgjegjësisë: Niveli GS-11 është niveli më i lartë i përshkruar në standardin GS-802. Pozicionet në këtë nivel kryejnë punën e fushëveprimit të gjerë dhe kompleksiteti kërkon aftësinë për të interpretuar, përzgjedhur, përshtatur, dhe aplikuar shumë udhëzime, precedentë, dhe parimet inxhinierike dhe praktika që lidhen me fushën e specializimit. Puna gjithashtu kërkon që tekniku të posedojë dhe të aplikojë disa njohuri të lidhura me fushat shkencore dhe inxhinierike. Në këtë nivel, teknikët planifikojnë dhe kryejnë projekte të plotë apo studime të natyrës konvencionale që kërkojnë përshtatjen e pavarur të sfondit të të dhënave, të informacionit dhe interpretimit dhe përdorimit të precedentëve. Ata janë konfrontuar në mënyrë tipike me një sërë problemesh komplekse që bëjnë thirrje për gjykim të konsiderueshëm në arritjen e kompromiseve dhe vendimeve inxhinierike të shëndosha. Puna shpesh kërkon koordinim të vazhdueshëm me personelin në organizata të tjera që ka një rol të rëndësishëm në realizimin e projekteve.

Puna e kryer në mënyrë tipike nga kërkuesit është e krahasueshme në nivelin GS-11. Natyra e detyrave të tyre të rregullta dhe të përsëritura kërkon që ata të interpretojnë, të zgjidhin, përshtatin dhe modifikojnë parimet ekzistuese standarde inxhinierike dhe praktikat, precedentet, specifikimet teknike dhe procedurat standarde të vendosura nga selia e marinës, NAVSEA(Naval Sea Systems Command) dhe prodhuesit.

Në studimin tonë duhet patur parasysh se GS- 802-11 si protokoll ka kufizime në distance, rrjedhimisht do të na duhet t'i bëjmë më të shpeshta 'Qelizat'. Sidomos në rrugët që kanë trafik të dendur aplikimi i hierarkisë mund të sjellë ngatërime në këtë rast. Në këtë rast shtimi i CC, do të sillte kosto më të madhe, ulje të probabilitetit dhe shpeshtësisë së shkëmbimit të mesazheve.

Konkluzione: Pavarësisht nga kufizimet, mundësitë që të ofron ky protokoll rutimi janë më të mëdha se ato që mund të ofrojnë protokolle te tjera. Me këtë protokoll rutimi arrihet koha minimale e komunikimit me konsumin minimal të burimeve të rrjetit, si dhe merret parasysh prezenca e zonave 'gri' përgjatë rrugës në të cilin mjeti lëviz.

Mendohet të ketë vështirësi në aksesimin e arkivave dhe dokumentacioneve reale të portit të Vlorës si dhe testimin real të protokollit. Megjithatë ashtu si në fushat e tjera të kërkimit shkencor ne do të përdorim simulimin. Do mundohemi të përdorim dy tipe të ndryshme në mënyrë që të bëjmë krahasimin. Gjithashtu si në analizë dhe në simulim do të përdorim krahasimin me protokolle të tjera ekzistues për komunikimet navale, sic është flooding(vërshimi/përmbytja).

KAPITULLI I:KOMUNIKIME INTER-NAVALE TË EMERGJENCËS. PROTOKOLLET E KOMUNIKIMEVE NDËR-NAVALE. VLORA RAST STUDIMI

Qëllimin e këtij kapitulli mund ta lidhim me sloganin: ***Siguri në det do të thotë të qëndrosh i lidhur, d.m.th komunikim pandërprerje në rrjet.*** Këtij qëllimi i vjen në ndihmë zgjedhja me kujdes e protokolleve të rutimit në komunikimet ndër- navale të emergjencës.

Shërbimet e navigimit në rastet e emergjencës mund të jenë një aplikim i rëndësishëm i rrjeteve sensor dhe ad-hoc wireless për shpëtimin dhe sigurimin e jetës së njerëzve. Si fillim në këtë kapitull do të flasim për sistemet IVC(Inter-Vehicular Comunication) dhe krahasimin mes tyre me MANETs, për sistemet dhe shërbimet që ndihmojnë në komunikimet ndër-navale, tipet e protokolleve që ndihmojnë komunikimet ndër-navale, do ndërtojmë një taksonomi të këtyre protokolleve të komunikimeve navale, dhe më pas do të diskutojmë mbi problemet që hasen gjatë komunikimeve ndër-navale dhe nevojën e tyre për protokolle të reja rutimi siç është edhe protokolli InterNavComm i propozuar nga ne.

1.1 Sistemet e Komunikimit Ndër-mjetore(IVC- Inter Vehicle Communication)

Anijet kanë pasur metodat e komunikimit brenda flotës që nga shfaqja e idesë që anijet të luftojnë si një forcë e bashkuar. Herët mesazhet janë përcjellë me anë të një sistemi të sinjaleve flamur, më pas me ndezje dritash. Me ardhjen e radios dhe komunikimit wireless komunikmi u bë më i thjeshtë. Me kalimin e kohës, sasia e informacionit që mund të transmetohet (pra bandwidth) është rritur, por ajo mbeti prapa te rrjetet tregtare. Ashtu si telefonat celulare dhe pajisjet e tjera mobile që u bënë të famshme, rrjetet e reja tregtare i ranë më shkurt, dhe para çdo publikimi ato vini në dispozicion të gjithë bandwidth_in duke tejkaluar atë që shumica e ushtrisë kishte në dispozicion. P.sh. për Marinën Amerikane, kjo ka qenë një pengesë e jashtëzakonshme për tu kapërcyer. Shqetësimi nuk është vetëm Bandwidth_i, por janë shqetësimet e sigurisë që çdo degë e ushtrisë ka kur përdor një rrjet mobile të aksesit publik. Marina gjithashtu përballet me pengesa shtesë të jo-çuditërisht pak kullave të operatorëve celularë në ujërat ku anije luftarake të mëdha janë në manovra. Kur

nuk ka asgjë mbi sipërfaqen e ujit, vetë anijet duhet të jenë kthyer në pikat e nevojshme rele/ritransmetuese. (Mihail L. Sichitiu, Maria Kihl, 2008)

Sistemet IVC mund të zbatohen ose, në disa situata, zëvendësohen me infrastruktura në anë të rrugës, duke lejuar akses interneti dhe një sërë aplikacionesh të tjera. Kohët e fundit termi rrjeti ad hoc i automjeteve (VANET) u prezantua për rrjetet multihop të automjeteve që nuk mbështeten në infrastrukturën në anë të rrugës. Në fakt termi IVC është më i përgjithshëm se VANET dhe përfshinë rrjetet e single-hop.

Në figurën 1.1 kemi paraqitur taksonominë e sistemeve të komunikimit të automjeteve. Ka tri tipe të mëdha sistemesh: sistemet IVC, sistemet RVC(roadside-to-vehicle communication) ku automejtet komunikojnë me sisteme në anën e rrugës dhe sistemet hibride të komunikimit mjetor (HVC).

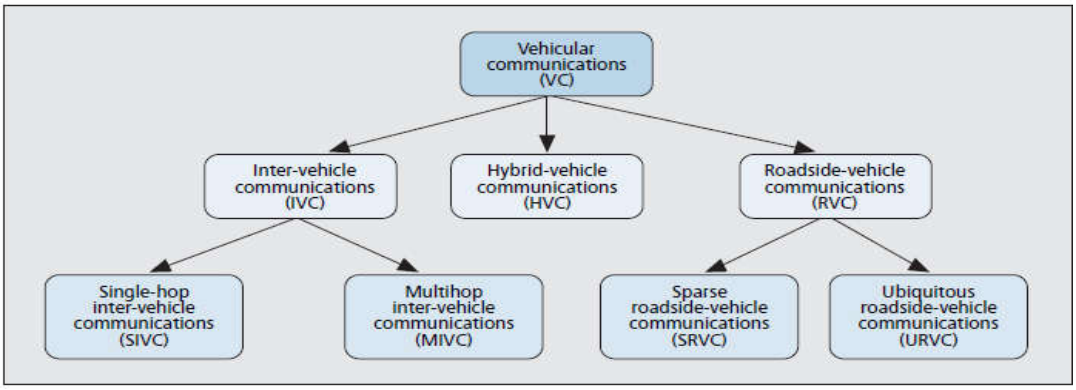


Figura 1.1 Një taksonomi e sistemeve të komunikimit mjetor. (Mihail L. Sichitiu, Maria Kihl, 2008)

- **Sistemet e komunikimit ndër- mjetor(mjet-me-mjet).** Sistemet IVC janë krejtësisht pa infrastrukturë; janë të nevojshme vetëm OBUs(onboard units) nganjëherë të quajtur edhe si pajisje në automje (IVE). Në varësi të faktit nëse informacioni është ritransmetuar në hop_et e ndërmjetme apo jo, mund të bëjmë dallimin ndërmjet IVCs single-hop dhe multihop (SIVCs dhe MICS).

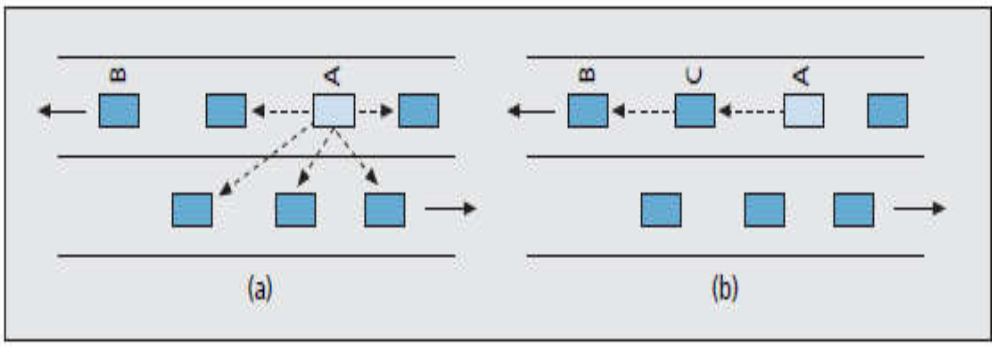


Figura 1.2 Sistemet IVC a) Single- hop b)Multihop (Mihail L. Sichitiu, Maria Kihl, 2008)

- **Sistemet e komunikimit mjet-me-rrugë** — Sistemet RVC supozojnë se të gjitha komunikimet bëhen ndërmjet infrastrukturës në anë të rrugës (duke përfshirë edhe njësitë në rrugë [RSUs]) dhe OBUs. Në varësi të aplikimit, dy lloje të ndryshme të infrastrukturës mund të dallohen, rrallë RVC (SRVC) dhe RVC (SRVC) sistemet e kudogjendur. Sistemet SRVC janë të aftë për ofrimin e shërbimeve të komunikimit në pika të nxehta. Një kryqëzim i zënë bënë caktimin e dritës së trafikut të vet, një stacion gazi reklamon ekzistencën e tij (dhe çmimet), dhe disponueshmëria e parkimit në një aeroport, janë shembuj të aplikimeve që kërkojnë një sistem SRVC(single hop). Një sistem SRVC mund të vendoset gradualisht, duke mos kërkuar investime të konsiderueshme para çdo përfitim në dispozicion. Një sistem UVC është Grail i shenjtë(holy grail) i komunikimit midis automjeteve: duke siguruar të gjitha rrugët me komunikim me shpejtësi të lartë do të mundëson aplikacionet të padisponueshme nga ndonjë sistem tjerër. Për fat të keq, një sistem UPVC mund të kërkojë investime të konsiderueshme për sigurimin e mbulimin e plotë (bile të rëndësishëm) të rrugëve ekzistuese (veçanërisht në vendet e mëdha si Shtetet e Bashkuara). (Mihail L. Sichitiu, Maria Kihl 2008)
- **Sistemet Hibride të Komunikimit ndër-automjetor(automjet me automjet):** sistemet HVAC janë propozuar në literaturë për zgjerimin e gamës së sistemeveve RVC. Në HVAC Sistemet e automjeteve komunikojnë me infrastrukturën në anë të rrugës, bile edhe kur ata nuk janë në rangun e drejtpërdrejtë wireless, duke përdorur automjete të tjera si rutera mobile. Një sistem HVC mundëson të njëjtat aplikime si

një sistem RVC por me një gamë më të madhe transmetimi. Avantazhi kryesor është se ai kërkon më pak infrastrukturë rrugore. Megjithatë, një disavantazh është se lidhja e rrjetit mund të mos jetë e garantuar në skenarë me densitet të ulët të automjeteve.

1.1.1 IVCs VS. MANETS

Ashtu siç mund të kemi theksuar edhe në kapitujt e mëparshëm, MANETs janë rrjetet wireless multihop që nuk kanë infrastrukturë, dhe janë të decentralizuar dhe të vetë-organizuar. Sistemet IVC plotësojnë të gjitha këto kërkesa, dhe për këtë arsye janë një klasë e veçantë e MANETs. Megjithatë, ka disa karakteristika që e diferencojnë IVCs nga supozimet e zakonshme të bëra në literaturën mbi MANETs:

- **Aplikimet:** Ndërsa shumica e artikujve të MANET nuk adresojnë aplikacione specifike, supozimi i zakonshëm në literaturën MANET është se aplikacionet MANET janë identike (ose të ngjashme) me ato të mundësuar nga Interneti. Në të kundërt, siç është treguar më vonë, IVCs kanë aplikime krejtësisht të ndryshme. Një pasojë e rëndësishme e diferencës në aplikimet është dallimi në mënyrat e adresimit.
- **Adresimi**. Në ngjashmëri të modelit të internetit, aplikimet MANET kërkojnë adresimin fiks pikë-me-pikë (unicast); ku, marrësi i një mesazhi është një tjetër nyje në rrjetin e përcaktuar nga adresa IP e vet. Megjithatë, aplikimet IVC shpesh kërkojnë shpërndarjen e mesazheve në nyje të shumta (multicast) që përmbushin disa kufizime gjeografike dhe ndoshta dhe kritere të tjera (psh, drejtimi i lëvizjes). Nevoja për këtë mënyrë adresimi kërkon një paradigmë rutimi të konsiderueshme të ndryshme.
- **Shkalla e ndryshimeve të Link_ut.** Në MANETs nyjet supozohet të kenë lëvizje të moderuar. Ky supozim u lejon protokolleve të rutimit MANETt (psh, Ad Hoc On Demand Distancë Vector, AODV) krijimin e pathe_ve pikë me pikë pathet që janë të vefshme për një kohë të arsyeshme dhe vetëm herë pas here kanë nevojë për riparime. Në aplikacionet IVC është treguar se për shkak të shkallës së lartë të lëvizshmërisë së nyjeve të përfshira, edhe path_et multi hop që përdorin vetëm nyjet

që lëvizin në të njëjtin drejtim në një autostrade kanë një jetëgjatësi të krahasueshme me kohën e nevojshme për të zbuluar path_in.

- **Modeli i Lëvizshmërisë.** Në MANETs, treguesi i rastit (RWP) është (deri tani) modeli më i shpesht i mobilitetit i përdorur. Megjithatë, për sistemet e IVC, një pjesë e mirë e kërkimeve ekzistuese njohin se RWP do të jetë një përafrim shumë i varfër i mobilitetit të vërtetë të automjeteve, në vend të kësaj, simulatorë të detajuara të trafikut të automjeteve përdoren.
- **Efikasiteti i energjisë.** Ndërsa në MANETs një pjesë e rëndësishme e literaturës ka të bëjë me protokollet efikase të energjisë, IVC gëzon një furnizim praktikisht të pakufizuar të energjisë.

1.2 Shërbimet e Komunikimit-Navigacional.

Përparim i shpejtë teknologjik në komunikimin hapësinor dhe kombinimi i navigimit me rritjen e kërkesave rregullatore të tij dhe presioni për të ulur koston kanë hapur mundësi të reja dhe emocionuese komerciale.

Për të ushqyer një popullsi në rritje të shpejtë në botë, njeriu gjithnjë e më tepër shikon në oqeane për ushqim dhe për ushqyerje. Si rezultat, problemi i mbi-peshkimit bëhet gjithnjë e më urgjente për tu zgjidhur. Aktiviteti i qëndrueshëm detare është bërë tashmë jetik për ekonominë globale.

Përveç kësaj, siguria është një shqetësim i vazhdueshëm dhe në rritje. Për të mbrojtur korsitë vitale të anijeve dhe ekonominë globale, agjencitë qeveritare mbështeten në shërbimet e monitorimit të anijes për të mbrojtur Zona Ekonomike Ekskluzive (EEZ). Bizneset tregtare gjithashtu gjurmojnë anijet e tyre që tu garantojnë siguri dhe mbrojtje kundër humbjes së pasurive të vlefshme. Sistemet satelitore të navigimi dhe komunikimit international (ICON) ofrojnë subjekte publike dhe sipërmarrje komerciale me aftësinë për monitorim efikas dhe përgjigje efektive për aktivitetin e anijes.

1.2.1 Sistemet Satelitore ICON

Sot, komunikimi globale për zonat e thella është një karakteristikë e mirë-krijuar e shërbimeve satelitore. Përveç kësaj, Global Navigation Satellite Systems (GNSS) mundësojnë ndjekjen globale të pasurive mobile. Sistemet satelitore ICON në mënyrë të përsosur integrojnë komunikimin satelitor dhe të navigacionit për të siguruar një shërbim të ri për të përmbushur nevojat e komunitetit detar.

Sistemet satelitore ICON do të sigurojnë një sistem global komunikimi hapësinor me shërbime survejimi me vlerë të shtuar për ndjekjen/gjurmimin e anijeve në të gjithë botën dhe një zgjidhje pikë me pikë(end-to-end) për gjurmimin e aseteve dhe menaxhimin e flotës, pozicionimin dhe ndjekjen, dërgimin e mesazheve dhe sigurinë për të gjitha llojet e anijeve në det përmes komunikimeve satelitë gjeostacionar Inmarsat dhe dy mikro-satelitëve në orbitë të ulët të Tokës për të siguruar mbulimin e rajoneve polare. Kjo do të rrisë sigurinë në rajonet detare, do të mundësojë menaxhimin efikas të flotave të peshkimit dhe do të kontribuojë në zhvillimin e qëndrueshëm të burimeve detare. Shërbimi punëson një mjet bazuar në terminalin e përdoruesit për të dërguar dhe për të marrë pozitën e lundrimit dhe informacione të tjera, si pjesë e mesazheve dixhitale. (SpaceTech7, Delft University of Technology Delft, The Netherlands, June 2005). Shërbimet e siguruara nga Sistemet Satelitore, janë paraqitur në tabelën 1.1si më poshtë.

Tabela 1.1. Shërbimet e siguruara nga Sistemet Satelitore ICON:

Shërbimi Bazë	Përshkrimi
Monitorimi i Mjetit	Transferimi automatik i rregullt i të dhënave të lundrimit të anijes dhe identifikimi.
Two-way Messaging[7]	Shkëmbimi i mesazheve të shkurtër ndërmjet përdoruesit detar dhe atij tokësor.
Ditar udhëtimi elektronik	Raportimi i aktiviteteve në bord, psh sasia e peshkut të kapur, përmes formave të paracaktuara.

[7] Njoftim dy –mënyrësh/krahësh

Geo-Fencing Alarm	Sigurimi i mesazheve të alarmit pasi zona të kufizuara janë shkelur/cënuar
Njoftim Alarmi/fatkeqësie	Transmetimi i mesazheve alarm nga një anije ne pritje të mesazhit të pranimit/njohjes

Sistemet satelitore ICON kanë krijuar një arkitekturë misioni të integruar që do të mundësojë një shumëllojshmëri shërbimesh për të përmbushur nevojat e tregut. Kjo arkitekturë përbëhet nga tri pjesë kryesore: segmenti i përdoruesit, segmentit i hapësirës dhe segmenti terren. Një segment përdoruesi përbëhet nga të gjithë terminalet e Sistemeve Satellitore ICON në bordin e anijes. Segmenti hapësirës është i përbërë nga Inmarsat dhe 'Mikro-satelitët që i përkasin Sistemeve Satelitore ICON. Së fundi, segmenti terren përfshin Qendrën e Shërbimit të Sistemeve Satelitore ICON si dhe ndërfaqe të Inmarsat.

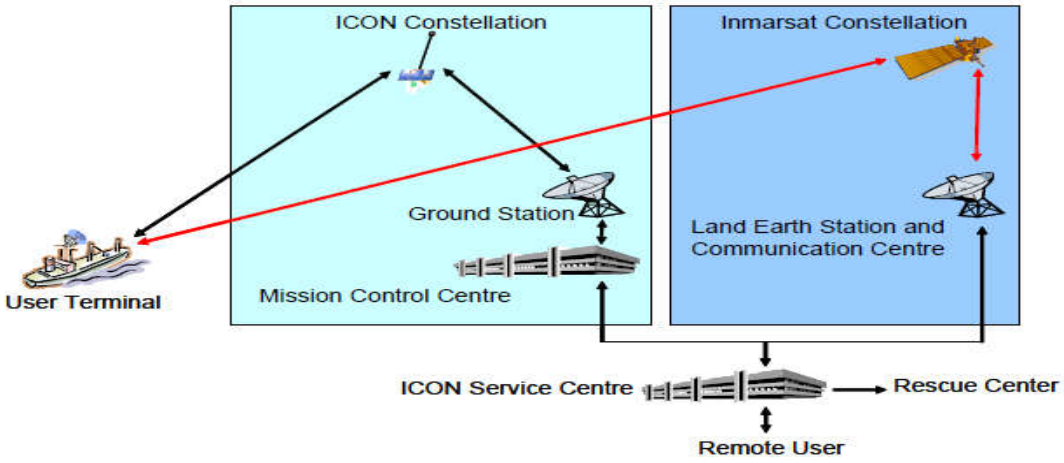


Figura 1.3 Arkitekturë e Integruar që mundëson një shumëllojshmëri shërbimesh(SpaceTech7, June 2005)

- **Shërbimet e Sistemeve Satelitore ICON**

Në bazë të një ankete të gjerë të klientit, sistemet satelitore ICON kanë zhvilluar shërbimet modulare të përshtatura për nevoja specifike. Këto përfshijnë: Distress Messaging(dërgimi mesazheve të fatkeqësive ose shqetësuese), Vessel Monitoring(Monitorimi i Mjetit), Geo-

Fencing Alarm(Alarmi Geo-Fencing), Two-Way Messaging(Two-Way Mesazhimi) dhe Electronic log-book(libër logimi elektronik). Më poshtë kemi përshkruar vetëm dy prej këtyre shërbimeve modulare: Vessel Monitoring dhe Two -Way Messaging.

Ky koncept i shërbimit modular në të ardhmen do të lehtësojë shtimin e shërbimeve të tilla si raportimi i motit te anijet ose shërbimet e SCADA(Supervisory Control and Data Acquisition).

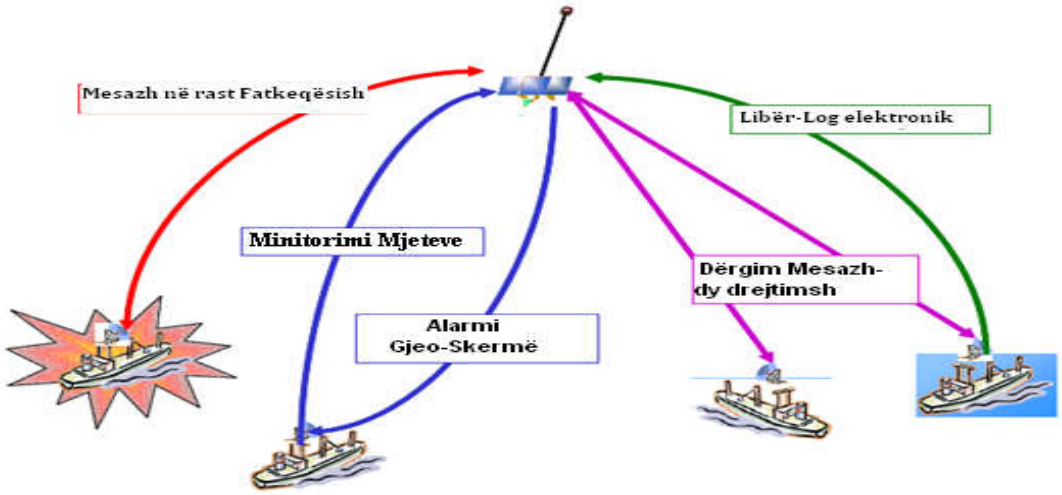


Figura 1.4 Disa Shërbime te Sitemeve Satelitore ICON (SpaceTech7, June 2005)

- **Monitorimi i Mjeteve dhe Two-Way Messaging[8](Rast Studimi Porti i Vlorës)**

Mesazhet dy drejtimshe mund të kryejnë njëkohësisht shkëmbimet anije-me-anije dhe anije-me-breg. Në intervale të rregullta, sistemi i monitorimit të anijes automatikisht transferon navigimin e sigurtë të mjetit dhe identifikimin e të dhënave për te qendra e shërbimit të sistemeve satelitore ICON. Duke iu referuar edhe figurave duhet patur parasysh që:

[8] Kalimi i mesazheve dy-drejtimësh

Figura 1.5 Mesazhet dy drejtimshe në shkëmbimet *anije-me-anije*.(Brigjet e Detit Adriatik, Vlorë, Anije të Bazës së Pashalimanit)

Figura 1.6 Mesazhet dy drejtimshe në shkëmbimet *anije-me-breg*.(Porti i vjetër në Vlorë)

- Shkëmbimi i mesazheve anije-me-anije ofron një komunikim të lehtë, të rehatshëm dhe të sigurt ndër-anijor, pa ndërprerë operacionet rutinë. (Fig.1.5)
- Në shkëmbimin e mesazheve anije-me-breg përdoruesi terminal komunikon me një përdorues tokësor nëpërmjet Qendrës së Shërbimit ICON Satellite Systems.(Fig.1.6)

- Shkëmbimi i mesazheve dy drejtimshe mundëson komunikimin ndërmjet përdoruesve gjeografikisht të largët dhe ofron komunikim të zgjeruar për rojet bregdetare dhe agjencitë e peshkimit.

1.2.2 Rrjetet Celular

Një rrjet celular është një rrjet komunikimi, ku hallka e fundit është pa tel. Rrjeti është i shpërndarë mbi zonat tokësore të quajtura qeliza, ku secila lidhet me një lokacion marrës fiks, i njohur si një site i qelizës apo stacion bazë.

Figura 1.7. Si punon një rrjet celular

Në figurën 1.7, më lartë tregohet qartë se stacioni bazë siguron qelizën me mbulimin e rrjetit i cili mund të përdoret për transmetimin e zërit, të të dhënave, etj... Një qelizë mund të përdor një grup të ndryshëm frekuencash nga qelizat fqinje, për të shmangur ndërhyrjen dhe për të siguruar cilësinë e shërbimit të garantuar brenda çdo qelize. Kur bashkohen së bashku këto qeliza sigurojnë mbulim radio mbi një zonë të gjerë gjeografike. Kjo mundëson një numër të madh të transceivers [9] portativ (p.sh., telefonat celularë, faqet, etj) për të komunikuar me njëri-tjetrin dhe me transceivers fikse dhe telefona kudo në rrjet, nëpërmjet stacioneve bazë, edhe në qoftë se disa nga transceivers lëvizin përmes më shumë se një qelize gjatë transmetimit.

[9] Marrës-transmetuesa

Arkitektura e përgjithshme e një rrjeti celular është e përbërë nga:

- **Mobile Station (MS) :** Stacioni celular-Baza e telefonisë celulare
- **Base Station (BS):** Stacioni bazë i cili është i lidhur me telefoninë celulare/stacionin celular përmes një ndërfaqe grafike.
- **Mobile Switching Centre (MSC):** qendra mobile e ndryshimit/kalimit e cila kontrollon një numër të caktuar qelizash(cluster_a), duke organizuar stacionet base dhe kanalet per rrjetet celulare dhe lidhjet e trajtuara.
- **National Carrier Exchange:** Kjo është porta drejt PSTN(Public Switched Telephone Network) nacionale fikse. Shpesh është e integruar me MSC(Mobile Switching Centre).

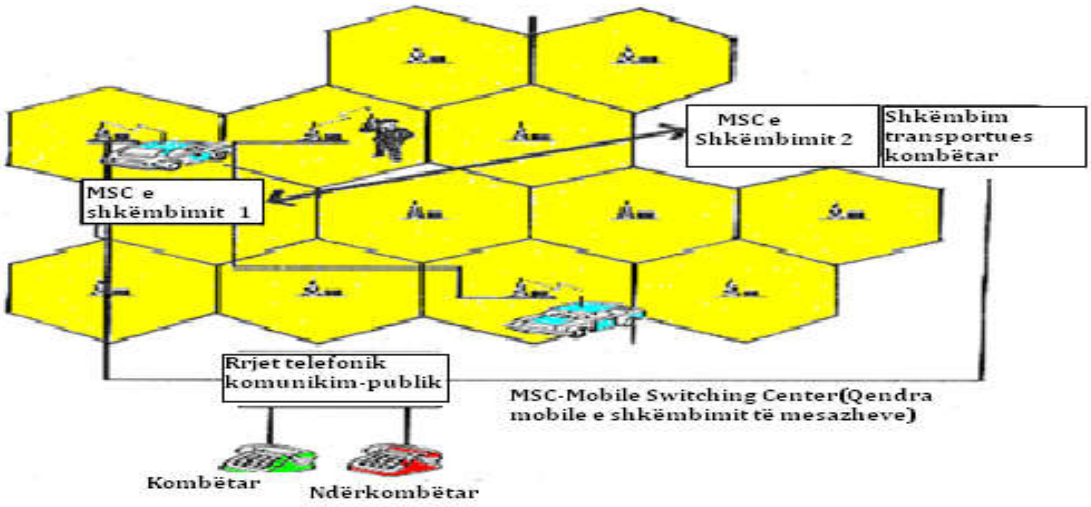


Figura 1.8. Shërbimi Kombëtar Transportues(National Carrier Exchange)

Rrjetet celulare ofrojnë një numër karakteristikash të dëshirueshme:

- Më shumë kapacitet se një transmetues i vetëm i madh, pasi e njëjta frekuencë mund të përdoret për lidhje të shumta për sa kohë që ato janë në qeliza të ndryshme.
- Pajisjet mobile përdorin më pak energji se sa një transmetues i vetëm ose satelit meqë kullat e qelizave janë më afër.

- Zonë më e madhe mbulimi se sa një transmetues i vetëm tokësor, pasi kullat shtesë celulare mund të shtohen në një kohë të pacaktuar dhe nuk janë të kufizuara nga horizonti.

Ofruesit më të mëdhenj të telekomunikacionit kanë vendosur rrjetet e zërit dhe të të dhënave celulare mbi pjesën më të madhe të zonës së banuar të Tokës. Kjo lejon telefonat celularë dhe pajisjet e lëvizshme informatike të lidhen me rrjetin telefonik publik dhe internetin publik. Rrjetet celulare private mund të përdoren për hulumtime ose për organizata të mëdha ose në flotë, të tilla si dërgimi për agjencitë vendore të sigurisë publike apo i një kompanie taksi.

Megjithatë siç mund të kemi theksuar më parë(tek hyrja) edhe këto tipe rrjetesh kanë problemet dhe limitet e tyre, sidomos në sinkronizime dhe problemet me multipath.

Limitimet:

Po nëse …

- nuk ka Infrastrukturë në dispozicion? -P.sh., Në zonat e fatkeqësisë
- ndoshta është shumë i shtrenjtë / i papërshtatshëm për tu ngritur? –P.sh., Në largësi, e site me konstruksion të madh.
- nuk ka kohë për ta vendosur atë? -P.sh., Në operacionet ushtarake

Të gjitha këto janë probleme për tu zgjidhur.

1.2.3 Sistemi Automatik i Identifikimit, AIS

Sistemi Automatik i Identifikimit (AIS) është një sistem automatik i pavarur për shkëmbimin e informacionit lundrues ndërmjet anijeve të pajisura në mënyrë të përshtatshme dhe stacioneve bregdetare duke përdorur mesazhe të qarta dhe operon në dy kanale VHF detare të përcaktuara. (Të dhëna të arshivuara të marra nga Marina: “Reparti Delta Forcë për kufirin dhe Migracionin Vlorë”, Porti i Vjetër Vlorë)

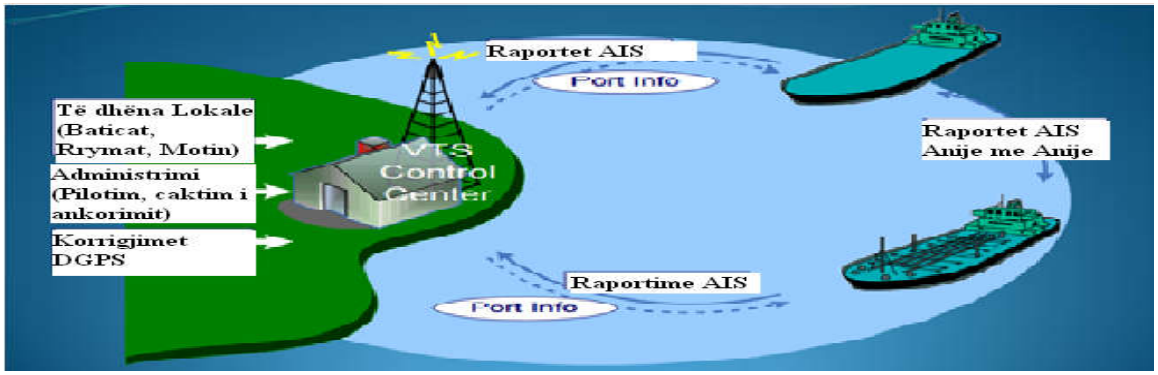


Figura 1.9. Sistemi AIS ndihmesë në Navigim dhe në Aeroplanë(SAR Aircraft)

Ky sistem punon mbi parimin bazë të transferimit të të dhënave në mënyrë elektronike në lidhje me një frekuencë radio valë. Një pajisje AIS përbëhet nga frekuenca shumë të larta (VHF) të transmetuesve dhe marrësve. Transmetuesi dhe marrësi i bashkëngjiten ekranit dhe sistemeve sensorë të anijes nëpërmjet një lidhje komunikimi. Për të marrë informacion të saktë të anijeve të tjera dhe gjithashtu për të dërguar vetë-informacionin e saj, AIS gjithashtu ka një sistem të pozicionimit global (GPS), i cili është i lidhur me një satelit. GPS mund të jetë një pajisje e brendshme e bashkangjitur ose një sistem i pajisur veçmas. AIS është i lidhur edhe me të gjitha sistemet e tjera të anijes dhe kjo është se si ajo merr të dhënat e anijes dhe i dërgonë ato në anije të tjera.

AIS është i njohur edhe si sistemi më i rëndësishëm dhe më i sigurtë i navigimit në bordin e një anije. Siç tregohet edhe në figurën 1.10, a dhe b, më poshtë:

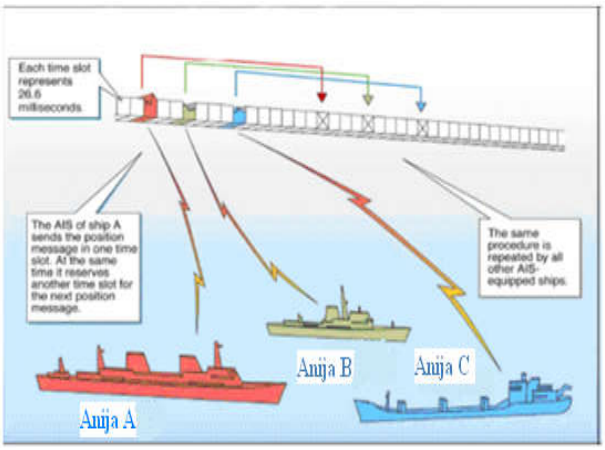


Figura 1.10. a)Parimi i punës së një AIS, b) AIS i integruar në anije

Kjo është për shkak se AIS punon automatikisht dhe vazhdimisht, duke dërguar dhe marr informacione pavarësisht nga pozita e anijes në lidhje me bregun. Për më tepër, edhe pse vetëm një kanal është i nevojshëm për të transferuar të dhënat, AIS ka gjithashtu një kanal të mesëm për të parandaluar çdo lloj ndërhyrje apo humbje të informacionit.

Gjithashtu, pasi secili prej anijeve ka sistemin e vet AIS, ekziston mundësia e lartë e rritjes së trafikut dhe bllokimit në kanalet. Megjithatë, kjo nuk ndodh kurrë. Sistemi AIS ka një sistem automatik që të zgjidhë pengesat midis vetes dhe stacioneve të tjera në dritën e rritjes së ngarkesës. Kjo është e mundur për shkak se çdo stacion ka slot(vendin e vet) e tij të transmetimit. Secili prej slot_eve është rreth 26.6 milisekonda, që do të thotë se çdo stacion mund të transmetojë informacionin gjatë asaj shumë kohë para se shansi të shkoj në stacionin e ardhshëm. Për këtë, ka gjithsej 2,250 sllot_e. Informacioni i dërguar nga një stacion në një slot të caktuar kohe shërben si referencë për informacionin e ardhshëm që vjen i cili ruhet në një slot tjetër të organizuar në mënyrë të rastësishme. Informacioni i marrë dhe i transmetuar nëpërmjet këtyre sllot_eve i transferohet menjëherë çdo automjeti i cili vjen në të njëjtën rang- radio. Kështu 2250 sllot_e të gjithë së bashku do të shërbejnë si një rrjet i përbashkët për të siguruar informacion për të gjitha anijet që vijnë nën kanalin e frekuencave të veçanta.

1.3 Problemet në Komunikimet Ndër-Navale dhe Nevoja për Protokolle të reja.

Siguri në det do të thotë të qëndrosh i lidhur në rrjet. Edhe pse çdo gjë në varkën tuaj është e ruajtur mirë dhe në gjendje të mirë pune, ju do të jeni i sigurt nëse ju jeni të siguruar, dhe kjo do të thotë marrje e informacionit të duhur të lundrimit, kur dërgoni një sinjal në rast emergjence .

Shumë probleme dhe situata si:

- trafiku i lartë
- moti i keq,
- emergjencat shëndetësor,
- urgjenca të tjera

- në anën tjetër shumicën e kohës nuk ka Wi-Fi ose mbulim tjetër, edhe nëse ajo është se nuk ka cilësi të mirë pritje për shkak të relievit dhe motit.

rrisin nevojën për përmirësime në komunikimet ndër-detare.

1.3.1 Komunikimi Anije –Breg

Komunikimi i të dhënave dhe zërit janë në dispozicion ndërmjet anijeve dhe bregut. Këto ndryshojnë nga koha në kohë si përmirësimi i teknologjive dhe lindin shumë plane të shërbimeve me kosto efektive *Komunikimet e-mail dhe aksesi web në det:* E-mail është në dispozicion në një bazë të afërt në kohë reale 24 orë në ditë dhe është metoda primare dhe e preferuar e kontaktit për qëllime personale dhe të biznesit.

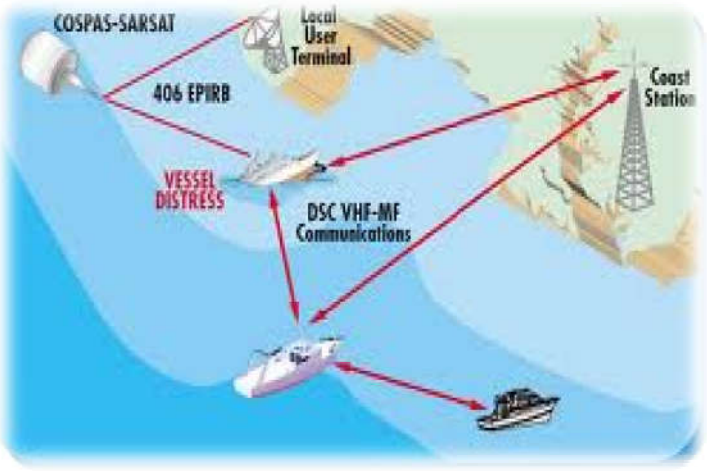


Figura 1.11 Komunikime Breg- Anije

Komunikimet broadband të internetit janë kryer nga kërkimet e anijeve nga Scripps[10]-që operon në det me anë të disa satelitëve të pavarur dhe sistemeve celulare. Në det të hapur, sistemi primar është Scripps HiSeasNet, i cili siguron lidhje pothuajse të vazhdueshme të internetit në mbarë botën.

Scripps është një nga qendrat më të vjetra, më e madhe dhe më e rëndësishme për marinën dhe hulumtimin shkencor në tokë, arsimin dhe shërbimin publik në botë. Epërsia e saj në det, tokë, dhe shkenca atmosferike është reflektues i programeve të tij të shkëlqyer, të fakultetit dhe shkencëtarëve të shquar kërkimore, dhe lehtësira të pazgjidhura.

[10] Scripps është një nga qendrat më të vjetra, më e madhe dhe më e rëndësishme për marinën dhe hulumtimin shkencor në tokë, arsimin dhe shërbimin publik në botë.

Gjithashtu duhet të theksojmë se përpos gjithë shërbimeve, shumë të mira e të dobishme që sistemet e komunimeve satelitore dhe ato të rrjetave mobile kanë në komunimet globale ato janë shpesh edhe subjekti i dështimit në det. Komunikimi nuk mund të ndodhë për shembull, kur pamja e antenës satelitore është bllokuar nga superstruktura e anijes, e cila ndodhet zakonisht në pjesën e bashit të anijes...

Problemet:

Tek komunikimet me Satelit ndeshen shpesh këto probleme:

- Kosto e lartë
- Brishtësi, dështime për shkak të infrastrukturës së anijes
- Vonesat
- Dështimi për të dërguar tekste të gjatë ose në imazhe për shkak të rënies/ndërprerjes së shkurtër në linkun satelit-anije.

Disa probleme tek Rrjetet Celular :

a) *Bandwidth të kufizuar* b) *Siguria*

Le të shohim në vazhdim se çfarë është bërë në këtë drejtim dhe çfarë duhet bërë, cili është propozimi ynë për të shmangur këto probleme:

- Naval Air Systems Command (NAVAIR) është duke testuar një program pilot. (WWAN) për të rritur komunikimet ekzistuese të bazuar në satelit. Rrjeti LTE (përdor 4G) lejon që personeli mbi dy anije të marrë në kohë reale video -streaming nga nyjet ajrore montuar mbi helikopter.
- Problemet: Kosto, Sigurimi, 4G(LTE(Long Term Evolution))

1.3.2 Komunikimi navigacional anije me anije shkon drejt 4G

Anijet kanë pasur metodat e komunikimit intrafleet[11] që kur doli ideja që mjetet të luftojnë si një forcë e bashkuar. Herët mesazhet përcilleshin me anë të një sistemi të

[11] Ndër-flot_ore

sinjaleve me flamuj, pastaj me ndezje dritash. Me shfaqjen e radios, e komunikimit wireless ishte më e thjeshtë.

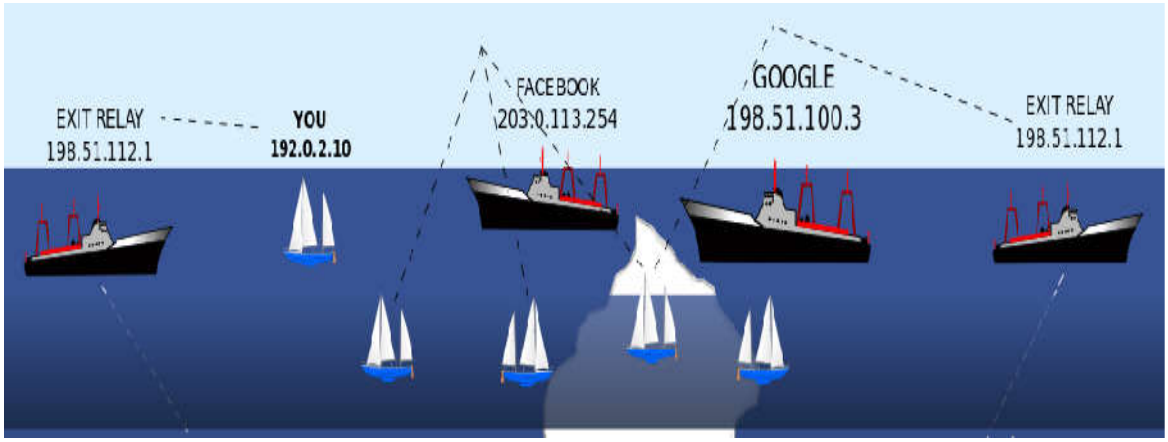


Figura 1.12. Komunikim Anije me Anije

Me kalimin e kohës, sasia e informacionit që mund të transmetohej(bandwidth) u rrit, por ajo mbeti prapa apo mbulonte më tepër rrjetet tregtare. Si telefonat celulare ashtu edhe pajisje të tjera mobile u bënë të famshme, rrjete te reja tregtare u shfaqen, dhe këtyre rrjeteve iu vendos në dispozicion Bandwidth i gjerë që tejkalonte edhe atë që shumica e ushtrisë kishte në dispozicion.

Për marinën e U.S, kjo ka qenë një pengesë e jashtëzakonshme për tu kapërcyer. Dhe nuk ka të bëjë vetëm me Bandwidth; ekzistojnë shqetësimet e sigurisë që çdo degë e ushtrisë ka kur përdor një rrjet celular publikisht të aksesueshëm. Marina gjithashtu përballet dhe me pengesa shtesë të jo çuditërisht pak antena të operatorëve celularë në ujërat ku luftanije të mëdha ndodhen në manovra. Kur nuk ka asgjë mbi sipërfaqen e ujit, por vetë anijet duhet të jenë kthyer në pikat e nevojshme rele. (Greg Crowe, GCN Magazine, 11 mars 2013).

Kjo është pikërisht ajo që Naval Air Systems Command (e NAVAIR) është duke bërë. Komanda ka testuar një program pilot në të cilën dy anije, USS Kearsarge dhe USS San Antonio, janë të pajisur me një rrjet me zonë të gjerë mikrovalë wireless (WWAN) për t'ia shtuar komunikimeve ekzistuese satelitore. Rrjeti LTE i i lejon personelit që ndodhet në dy anije të marrë në kohë reale video streaming nga nyjet ajrit montuar në

helikopterët, e cila nga ana e vet i lejon oficerët që të marrin vendime më shpejt dhe më të sakta bazuar në atë që paraprakisht njësitë janë bërë. (Greg Crowe, GCN Magazine, 11 mars 2013).

Larry Hollingsworth NAVAIR drejtor kombëtar për aviacionin R & D tha: "LTE i lejon NAVY të drejtoj të gjitha avantazhet e telefonat smart dhe broadband komerciale". "NAVAIR po përpiqet të trajtojë një kërkesë kritike për misionin VBSS [Vizita, bordi, kërkimi dhe konfiskimi], por përveç kësaj marinarët tashmë kanë gjetur rrjetin e tyre të dobishme në punën e tyre të përditshme. Kjo ka kuptim të përbashkët, pasi edhe pse ne të gjithë e përdorim teknologjinë e telefonit smart në jetën tonë personale, nuk është befasuese se marinarët do ta shtrinë atë gjë të dobishme për punën e tyre.

LTE, zakonisht emërohet si 4G LTE, është një standard për komunikimet me shpejtësi të lartë midis pajisjeve të lëvizshme, dhe i transmeton të dhënat në rreth 100 megabits / sek, me shpejtësinë e duhur për të trajtuar imazhet dhe videot si dhe zërin dhe tekstin. Në vitin 2012, policia në Florida testuar një rrjet i dedikuar LTE për të trajtuar sigurinë gjatë Konventës Kombëtare Republikane. Ekipet që u përgjigjen emergjencave në zonën e Denverit gjithashtu janë duke përdorur LTE për një rrjet të sigurisë publike.

Por çfarë është LTE dhe pse është i rëndësishëm për një rrjet të sigurt publik: Gjatë ngjarjeve të mëdha ne kemi vështirësi në përdorimin e telefonave tanë celularë për shkak të mbingarkesës në rrjet ", tha Moushon. Sepse rrjeti demo RNC nuk ka përdorur një bartës komercial dhe ishte dedikuar për policinë kur nuk kishte mbipopullim, duke i bërë shërbimet të avancuara që të vihen në dispozicion për komunikimet në misione-kritike. "Kjo ishte absolutisht e madhe për ne," tha ai. Sistemi 4G LTE(Long Term Evolution) vepron në Band 14 të rrjetit të sigurisë publike në rangun 700 MHz e broadband. Kjo është pjesë e një përpjekje për të siguruar responder-a e parë të rajonit me një teknologji që do të lejojë që ata të ndajnë komunikimin përtej kufijve juridiksionale, tha Frank Brzezinski, manaxher i zhvillimit të biznesit menaxher i divizionit i Sistemeve të Integruara të Raytheon, i cili instalon sistemin. (Nga William Jackson, Sep 17, 2012).

1.3.3 Komunikimet Littoral_e[12] Breg-Anije me mangësi, sipas GAO.

- GAO(Government Accountability Office) në kërkimet e saj së fundmi zbuloi se në sistemet e komunikimit mungon besueshmëria e nevojshme, shpejtësia dhe bandwidth_i.
- Ndërtimi i një infrasrukture për këto lloje komunikimesh rezulton shumë i shtrenjtë.

Anijeve Luftarake të Marinës të SHBA-së u mungojnë sistemet e fuqishme të komunikimit të nevojshme për të transmetuar të dhënat kritike për të mbështetur objektet në breg, sipas një auditimi të palëshuar të kongresit, i fundit në një varg të problemeve për programin e ndërtimit të anijeve është 34 milionë $.

Zyra e Llogaridhënies e Qeverisë Amerikane, në një përmbledhje të LCS, tha: Anijet e Lehta(me tonazh të lehtë) mbështeten në komunikimet anije-me-breg për të ndihmuar ekipet që monitorojnë gjendjen e anijes, kryejnë riparime dhe urdhërojnë furnizime mjekësore. Auditimi zbuloi se në sistemet e komunikimit mungon besueshmëria e nevojshme, shpejtësia dhe bandwidth.

Mangësitë e komunikimit i shtohen kritikave të mjetit/anijes, i cili ka për qëllim të jetë i vogël, i shpejtë, dhe i adaptueshëm për të patrulluar ujërat e cekëta pranë bregut në hapësira të tilla si të Gjirit Persik dhe Detit të Kinës Jugore.

Programi për të ndërtuar një total prej 52 anijesh në dy versione të bërë nga Lockheed Martin Corp dhe Austal Ltd është ballafaquar me një listë të zgjeruar të pyetjeve në lidhje me pozitat e tyre, armatimet/fuqi zjarri, mbrojtjen dhe mbijetesën edhe pse kostot e projektuara këtij ndërtimi e kanë kaluar parashikimin dhe Pentagoni përballet me shkurtime automatike buxhetore prej rreth 500 miliardë $, më shumë se gjatë një dekadë..

"Derisa sistemet e komunikimit dhe shqetësimet e Bandwidth janë adresuar plotësisht," aftësia e flotën "për të ndarë informacion me pajisjet mbështetëse në breg mund të jetë e kufizuar dhe mund të zvogëlojë disponueshmërinë operative të anijes," sipas raportit, të datës 9 Shtator të emërtuar "Për përdorimin zyrtar vetëm ", që është marrë nga Bloomberg News.

[12] Bregdetare

Auditimi GAO u bazua në vlerësimin e çështjeve të ngritura në katër raportime të brendshëm të Navy vitin e kaluar.

Përgjigja e NAVY[13]

Caroline Hutcheson Togere, një zëdhënëse e Navy, tha se "shumë përpjekje është bërë për të vlerësuar se si të përmirësohet Anija Luftarake Littorale", dhe "rekomandimet e GAO kanë qenë pjesë e diskutimeve të hollësishme se si Navy e vlerëson programin".

"Këshilli LCS i marinës, i formuar vitin e kaluar për të shqyrtuar programin" i është adresuar sistemeve të komunikimit të anijeve," tha Hutcheson në një e-mail. Ndërsa anijet kanë kapërcyer të metat e hershme, të tilla si çarjet dhe korrozionin, sipas GAO, ata përballen me pyetje të vazhdueshme, duke përfshirë aftësinë e tyre për të mbijetuar ndaj një goditje nga raketat kundër-anije.

Madje në rolin e tij të luftës të sipërfaqes, kur të gjitha sistemet e saj të armëve janë duke punuar si duhet, anija "është vetëm në gjendje të neutralizojë" anije të vogla të sulmit, si ato që Irani ka, dhe ajo "mbetet e pambrojtur ndaj anijeve" me raketa kundër-anije lundrimi që mund të udhëtojnë më shumë se pesë milje (8 kilometra), sipas një raporti të marsit të vitit 2012 të marinës.

Shkëmbimi i moduleve

Zyrtarët e marinës po ashtu kanë vënë në diskutim nevojën praktike të anijes 'për t'u kthyer në port për të shkëmbyer module të përshtatura për detyra të tilla si sipërfaqe luftarake, operacionet dhe misionet kundër - nëndetëse.

Dështim "katastrofikë"

Marina nuk e ka trajtuar plotësisht "pamjaftueshmërinë për të trajtuar të dhënat e rrjedhshme të vazhdueshme të nevojshme LCS" të një sistemit të madhë dhe nuk është "duke hetuar ose investuar në Bandwidth e sistemit të komunikimit dhe në tepricën e të dhënave që do të zbuste dështimin e sistemit," theksoi GAO.

[13] Marina

Zyrtarët e marinës njohën rëndësinë e komunikimit të besueshëm anije-me-breg në përgjigjen e tyre ndaj GAO, duke thënë se monitorimi efektiv i të dhënave të mirëmbajtjes së anijes "parandaloi një dështim katastrofik të sistemit" që i "lejoi marinës të marrë veprime lehtësuese dhe të shmang shpenzimet e mëdha." (Tony Capaccio , November 19, 2013)

1.3.4 Komunikimet Littoral_e[14] Breg-Anije me mangësi, të dhëna nga portet e Vlorës.

Sipas një inerviste që patëm me komandatin dhe teknikë të bazës së Policisë Detare, Vlorë por edhe me personat kompetentë që takuam në Portin e Vjetër, Vlorë u vërejt qartë nevoja e ekzistencës së komunikimeve të sigurta.
Madje nga një anlizë aktuale mbi komunikimin rezultonte që të gjitha skafet policore detare si dhe anijet e peshkimi dhe anije të tjera pasi kalonin Karabrunin(mbas tij) kishin probleme me komunikimin, me antenat dhe radiot, madje na u deklarua se kishin shkëputje në komunikimin me bregun, pra nuk kishin më mbulim(s'ka valë), për të siguruar një komunikim normal, më poshtë janë dhënë koordinatat ku ndodhin këto shkëputje me bregun:

- Kanal Jug.Karaburun 40 27 76 N 87 19 17. E
- Kanal Veri.Karaburun 40,31 54 N 19 15 99 E

Por jo vetëm në këtë zonë, por edhe në dis azona të tjera si p.sh. në zonën midis Qeparoit(në fund të tij) dhe Borshit raportohen shpesh nga drejtuesit e mejteve raste të tilla për mungesë komunikimi apo mbulimi vale për të patur një komunikim normal mjet me breg.

Përsa i përket zonës së Vlorës në bazë të materialeve të mbledhura nga Porti i Vjetër dhe Porti i Policisë Detare mund të listojmë disa nga pajisjet që përdoren në skafet dhe anijet që navigojnë në ujrat e këtyre porteve por edhe nëpër anijet që navigojnë gjithë bregdetin tonë, të tilla janë: Radari- Furuno Universla AIS(Fa-150), NavNet 3D; Salor-radiolidhëse; Radio-Sepura; Navionics (Humminbird); Furuno FI-50. Le të trajtojmë shkurt secilën prej tyre, për tu njohur më mirë me komunikimin breg- anije; anije –anije:

[14] Bregdetare

Figura 1.13. Furuno Universal AIS(Fa-150)

FA-150 është një AIS universal (Automatic Sistemit të Identifikimit) për det të hapur dhe për rrugët ujore të njësive të brendshme/mbyllura, të aftë për të shkëmbyer të dhëna navigimi dhe të anijes ndërmjet anijeve të tjera apo stacioneve bregdetare. Është në pajtueshmëri me IMO MSC.74 (69) Aneksi 3, A.694, ITU-RM.1371-4 dhe DSC ITU-R M.825. Ajo gjithashtu është në përputhje me IEC 61993-2 (testimit Typestandard), IEC 60945 (EMC dhe kushtet mjedisore*)(informacione të marra nga manuale që dispononte Baza e Policisë Detare, Vlorë).*

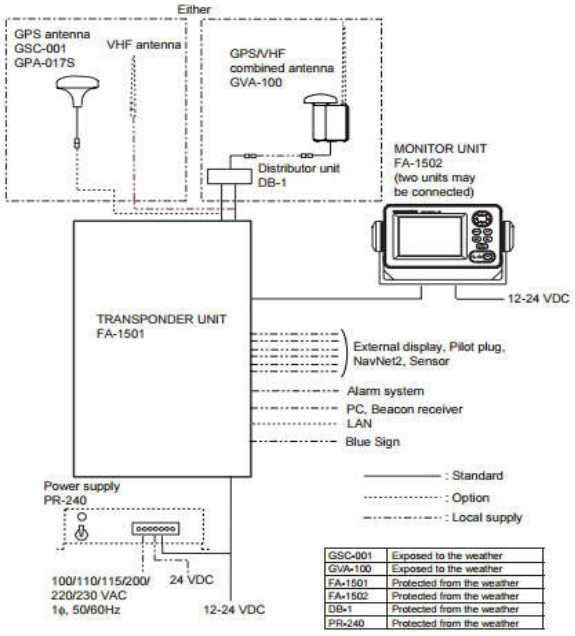


Figura 1.14. Sistemi i konfigurimit(marrë nga Baza e Policisë

Në Figurën 1.14 po paraqesim në mënyrë skematike **<u>Sistemin e Konfigurimit:</u>**

Sistemi i identifikimit Automatik (AIS) është zhvilluar fillimisht për të ndihmuar Vessel Traffic Services [15] (VTS) duke përdorur një transponder VHF që punon në Call Digital Selektiv (DSC) në VHF CH70, dhe është ende në përdorim përgjatë zonave bregdetare në UK dhe zona të tjera bregdetare. Disa

[15] Shërbimet e Trafikut të Anijes

kohë më vonë IMO zhvilloi një AIS universale duke përdorur teknologji të re të sofistikuar të quajtur Self-Organized Koha Division Multiple Access (SOTDMA) në bazë të të dhënave VHF Link (VDL).

Sistemi funksionon në tre mënyra – autonom (funksionimin e vazhdueshëm në të gjitha fushat), - në intervale të caktuara (transmetimin e të dhënave të kontrolluara nga distanca nga autoritet në shërbimin e monitorimit të trafikut) - dhe anketime (në përgjigje të pyetjeve nga një anije ose autoritet). Ajo është e sinkronizuar me kohën e GPS për të shmangur konfliktin ndërmjet përdoruesve të shumtë (IMO minimale 2000 Raporte për minutë dhe IEC kërkon 4500 raporte për dy kanale). Kanalet VHF 87B dhe 88B janë përdorur shpesh dhe përveç kësaj ka frekuenca lokal. Transponder_at AIS të anijes shkëmbejnë të dhëna të ndryshme siç përcaktohet nga IMO dhe ITU në ose frekuenca të krijuara automatikisht nga telekomandimi i menaxhimit të frekuencave pranuar nga marrësi DSC në anije.

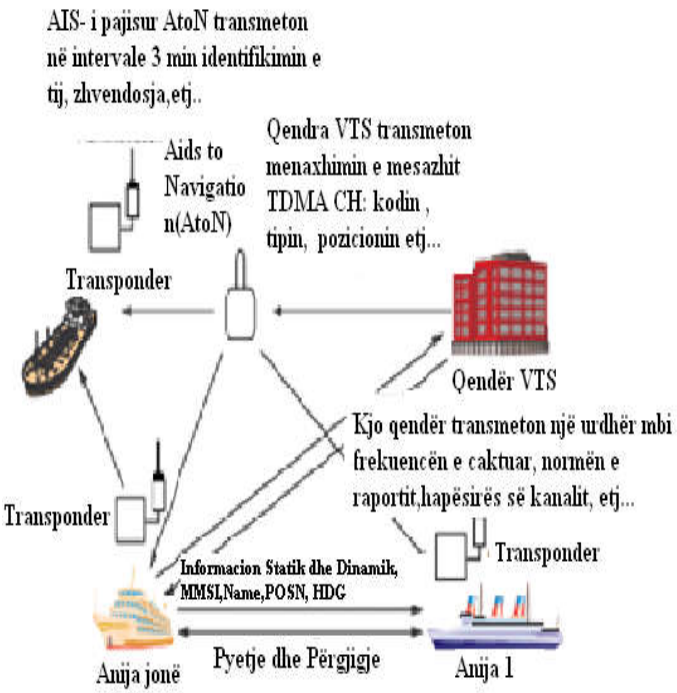


Figura 1.15 Sistemi AIS

Siç përmendëm më lartë pajisje të tjera të rëndësishme janë edhe NavNet 3D; Salor-radiolidhëse, në figurën1.16 paraqitet pamje nga porti i Policisë Detare, pamje të sistemit të drejtimit, të kabinës së mjeteve (skafeve) të policisë detare, si dhe pamje nga Navnet 3D, Furuno.

Furuno ofron një linjë të plotë të pajisjeve të komunikimit për të na mbajtur të lidhur me të tjerët, duke përfshirë AIS, Radiotelefonë një apo shumë stacionesh, marrës NAVTEX, faksimile të motit dhe stacione tokësore mobile Inmarsat. Gama e gjerë e pajisjeve të komunikimit u ofron dejtuesve të mjeteve të vogla të njëjtën cilësi dhe besueshmëri të zgjedhur nga komuniteti tregtar detar.

Figura 1.16. Porti i Policisë Detare pamje të sistemit të drejtimit, të kabinës së mjeteve (skafeve) të policisë detare.

Navnet 3D është një sistem novator navigacioni, që paraqet koncepte të reja për ndërfaqen e përdoruesit që e bën lundrimin në anijet tuaj më të lehtë se kurrë më parë.

Por çfarë protokoll komunikimi përdorin pjisjet e komunikimit të ndërfutura në anije, siç është AIS?

CAN bus është një protocoll komunikimi që ndan të dhënat e shumta dhe sinjale nëpërmjet një kabllo të vetme si shtylla kurrizore.

Ne thjesht mund të lidhim ndonjë pajisje CAN bus në pjesën kryesore të kabllit për të zgjeruar rrjetin tuaj në bord. Me CAN bus, ID janë caktuar në të gjitha pajisjet, dhe statusi i çdo sensori në rrjet mund të detektohet. Të gjitha pajisjet e CAN të mund të përfshihen në rrjetin NMEA 2000.

Të gjitha sensorë e radarit Navnet 3D inkorporojnë një port CAN bus tek e cila disa sensorë CAN bus mund të lidhen direkt. Fuqia për këto sensorë të rrjetit furnizohet direkt nga vetë radari. Ky tipar unik lejon instalim fleksibël të sensorë të shumfishtë, pa nevojën për të drejtuar kabllot gjatë gjithë rrugës për njësinë kryesore procesor. Të dhënat e CAN bus

konvertohen dhe shpërndahen kudo në rrjetin Navnet 3D Ethernet. Ku, Navnet 3D është e ndërtuar mbi një rrjet Ethernet, duke lejuar që të shtohen komponentë pak ose shumë sa një person mund të dëshirojë së bashku me deri në dhjetë ekrane për të krijuar një suitë të përsosur lundrimi.

Për më tepër, këto pajisje si NMEA 0183 dhe CAN bus mund të lidhen tek çdo ekran apo procesor BB dhe mund të ndajnë/përcjellin informacionin automatikisht në të gjithë rrjetin Ethernet. Të dhënat e vendosura nga përdoruesi gjithashtu mund të transferohen duke përdorur kartat SD për sinkronizimin e parametrave të operimit përmes shfaqjeve të rrjetit. Sinkronizimi i fuqisë on / off përmes të gjitha njësive të ekranit Navnet 3D mund të arrihet kur përdoret një hub i dedikuar HUB101 Ethernet. Sistemi Navnet 3D është ndërtuar mbi teknologjinë më të përparuar chart plotter[16].

Po të shtohet Radar UHD ™ dhe Fish Finder[17] FDF ™, së bashku me zgjedhjen nga një shumëllojshmëri e gjerë opsionesh sensorësh dhe deri në dhjetë ekrane. Përveç kësaj, NAVpilot i Furuno gjithashtu mund të jetë i lidhur me sistemin. Është e lehtë për të parë se si ekrani chart plotter bëhet Gjeneza e suitës më të sofistikuar të lundrimit në dispozicion.

Konfigurimi bazë i Navnet 3D na lejon të zgjedhim ose MFD12, 12.1 "Multi Function Display ose MFD8, 8" Multi Function Display. Mbi të gjitha, Navnet 3D ofron konfigurimin Blackbox me të cilat ju mund të përdorni Furuno e MU-seri 12.1/15/17 "LCD me ngjyra ose një monitor porosi deri në zgjidhjen e ekranit SXGA. Të gjitha kombinimet deri në 10 MFDs janë të mundshme në një rrjet Navnet 3D.

Numri maksimal i Sensore Radar Digital (DRS) në një rrjet maksimumi është deri në katër DRS dhe secili prej MFD8/MFD12/MFDBB ka një Hard Disk Drive (HDD) të brendshëm me 40 gigabajt të kapacitetit të hapsirës së kujtesës.

[16] Një chartplotter është një pajisje e përdorur në navigacion detar e cila integron të dhënat e GPS me një tabelë elektronike lundrimit (ENC).

[17] Një Fishfinder ose jehone është një instrument i përdorur për të gjetur peshk nënujë duke detektuar impulse të pasqyruara të energjisë së tingullit, si në sonar. A Fishfinder moderne paraqet matjet e tingullit të pasqyruara në një ekran grafik, duke lejuar një operator për të interpretuar informacionin për të gjetur grumbujt e peshkut, mbeturinat nënujore, etj...

MFD pranon një mouse USB që është mbështetur nga Generic USB Driver. Shumica e veprimeve janë të mundshme duke përdorur një mouse USB. Por a mundet që të dhënat e makinës të shfaqen në NMEA2000 dhe çfarë është një NMEA 2000? Po mund të pranohen nga NMEA 2000 i cili është një protokoll rutimi i NMEA që lehtëson komunikimin me shpejtësi të madhe të vëllimit të madh të të dhënave gjithashtu edhe shpërndarjen me lehtësi të rrjeteve të sistemit të navigimit.

Përveç 2 protokolleve të përmendura më sipër, që ndihmonin në komunikimin navigacional, në çështjen më poshtë do të trajtojmë edhe disa protokolle të tjera, të cilat mund të kenë të bëjnë me rutimin, efiçencën e energjisë, lokalizime, etj...

1.4 Një Vështrim i Përgjithshëm i Protokolleve në Komunikimet Inter-Navale. Konkluzione

1.4.1 Një Taksonomi Mbi Protokollet Ndërnavale

Pjesa më e madhe e protokolleve IVC(komunikimi ndërmjetor) përdorin përmbytjen (flooding) si rrugën më të thjeshtë për transmetimin(broadcast). Por flooding performon relativisht mirë për një numër të kufizuar të nyjeve, kjo performancë bie ndjeshëm nëse numri i nyjeve rritet. Kur secila nyje merr dhe transmeton mesazhin pothuajse në të njëjtën kohë, kjo shkakton konflikt dhe përplasje, stuhi transmetimi dhe konsumim të lartë të bandwidth_it.

Nëse do të bënim një ndarje apo klasifikim të këtyre protokolleve të cilat ndihmojnë komunikimet mjet me mjet, në rastin konkret anije me anije, do të listonim si më poshtë:

- Protokolle Ad hoc (të rutimit)
- Protokollet gjeografike të internetit
- Protokolle rutimi që kanë të bëjnë me efiçiencën e energjisë.
- Protokolle rutimi që kanë të bëjnë me lokalizime, etj...

Ashtu siç mund të kemi theksuar dhe evidentuar më sipër, komunikimi anije me anije (Ship-to-ship) kontribuon në krijimin e një rrjeti ad-hoc wireless. Protokollet Ad-hoc janë shumë të përshtatshme për t'u përdorur në port, pikërisht në fushën e komunikimit ndër-detare.

Prandaj dhe në këtë temë jemi fokusuar dhe kemi patur për qëllim pikërisht ndërtimin e një protokolli rutimi të përshtatshëm në komunikimet anije me anije, dhe me anë të cilit të rritet siguria e njerëzve dhe mjetit të lundrimit. Por për këtë protokoll rutimi do të flasim, do e shpjegojmë dhe do e trajtojmë më gjerë në kapitujt më poshtë.

Në këtë pikë do të ndalemi tek trajtimi i disa prej protokolleve të cilat bëjnë pjesë në taksonominë e paraqitur më poshtë, dhe që janë pikërisht ato protokolle që ndihmojnë në komikimet ndërnavale.

- **Protokolle të tjera që ndihmojnë komunikimet Navale:**

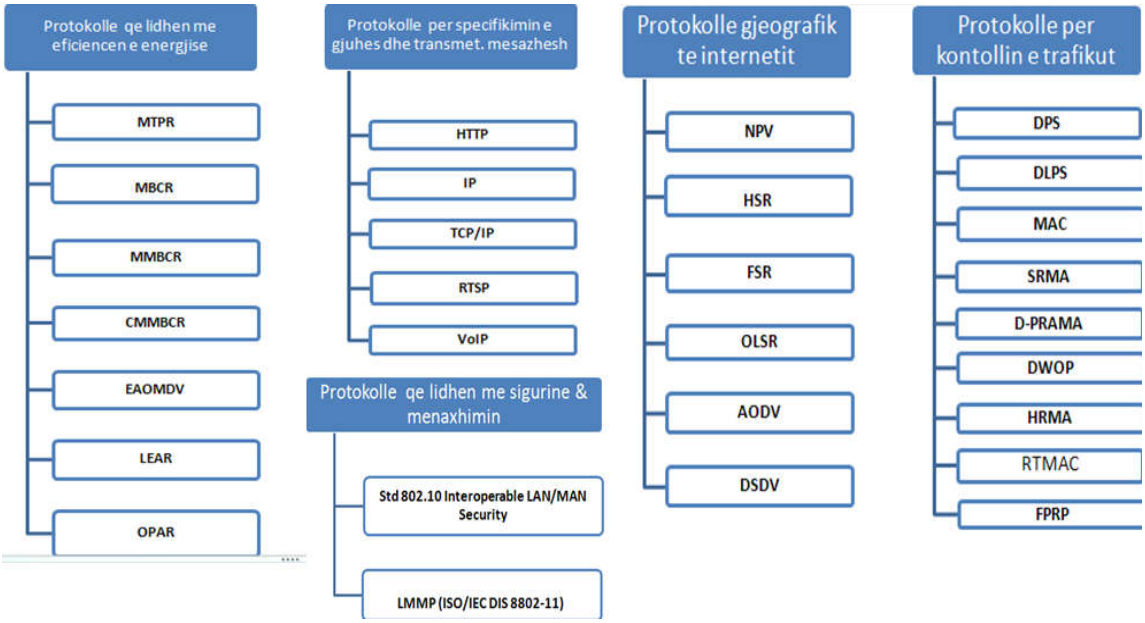


Figura 1.17. Taksonomi e protokolleve të komunikmeve ndërnavale

- **Protokolle që lidhen me efiçiencën e energjisë**

Siç mund të shihet edhe nga taksonomia e më sipërme kemi disa protokolle të cilat ndihmojnë në eficiencën e energjisë, le të trajtojmë disa prej tyre:

MMBCR(Min-Max Battery Cost Routing): Idea është që të kuptojmë se çfarë performance dhe funksionimi ka protokolli i rutimit i efikasitetit të Energjisë për rrjetin

mobile ad hoc. Analiza e këtij protokolli është bërë duke marrë një rrjet si shembulli në figurën më poshtë:

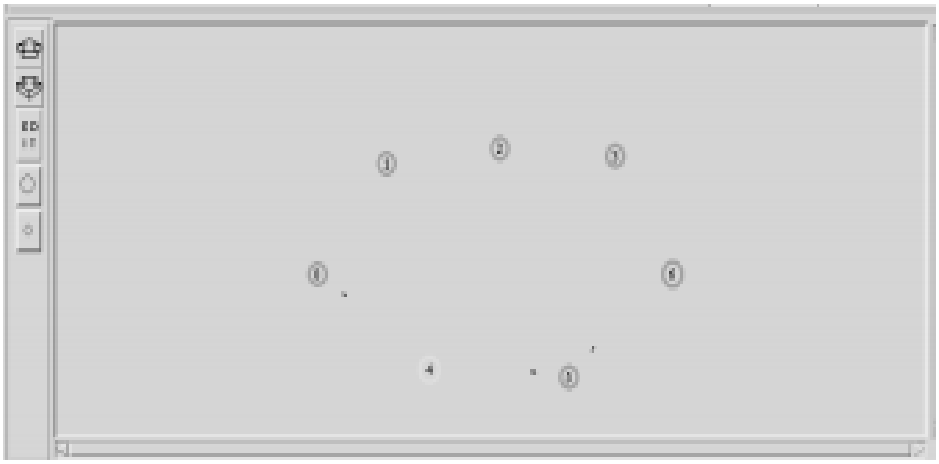


Figura 1.18. Një snapshot/fotografi që tregon rrugën 0-4-5-6 që është zgjedhur nga MBCR(marr nga faqe web)

Protokollet e eficiencës së Energjisë marrin parasysh energjitë e mbetura të nyjeve ndërkohë edhe përzgjedhjen e rrugës për në destinacion. Min-Max Battery Kosto Routing (MMBCR) së pari e gjen nyjen që ka kapacitet minimal të baterisë në secilën prej rrugëve të mundshme dhe përzgjedh rrugën që ka vlera maksimale midis rrugëve të zgjedhura. Kjo do të thotë se është zgjedhur rruga që ka jetëgjatësinë maksimale. Por e metë kryesore e MMBCR është se ajo nuk i konsideron fuqitë e e transmetimit të nyjeve. Në MMBCR, informacioni i përditësuar nuk konsiderohet për zgjedhjen e rrugës. Një problem tjetër në protokollin ekzistues MMBCR është se sapo rruga është zgjedhur në fazën e zbulimit të rrugëzimit, rruga e zgjedhur është përdorur deri sa të gjitha paketat e të dhënave dërgohen ose deri sa rruga e zgjedhur dështon për shkak të shkarkimit të baterisë së nyjes. Nëse ndonjë nga nyjet në rrugën e zgjedhur nuk ka energji të mjaftueshme, ato nyje me siguri do të vdesin duke shkaktuar dështimin e rrugëzimit dhe kështu jetëgjatësinë e përgjithshme të rrjetit. Këtu, nyjet në rrugën e zgjedhur pësojnë shumë në mënyrë të vazhdueshme për shkak të paketave që vijnë nga nyjet e tjera.

Sigurisht që për të rregulluar këto probleme janë propozuar mekanizma zbulimi te cilët rregullojnë disi proçesin e rrugëzimit. Por mendohet se ka akoma shumë për tu bërë në këtë drejtim, shanset e dështimit të link_eve janë të shumta.

MTPR(Minimum Total Transmission Power Routing): Protokolli MTPR është përdorur për të minimizuar konsumin e energjisë totale të transmetimit për komunikim multi-hop. Që fuqia e transmetimit është proporcionale me distancën e transmetimit midis dy nyjeve fqinje, pra MTPR protokoll gjithmonë zgjedh një rrugë me fuqi më minimale të transmetimit, por me më shumë Hop_e. Megjithatë, protokolli MTPR pëson gjatë vonesës end-to-end, pikërisht nga numri më i madh i Hop_ve.

Kufizimet:

- Vështirësia, në lidhje, me baterinë e mbetur të një nyje
- Numri i madh i nyjeve të 'Vdekura'
- Vonesa të mëdha end-to-end

LEAR (Local Energy Aware Routing)protocol): Është një protokoll i bazuar në mekanizmin DSR të rutimit. Ideja kryesore e LEAR është të marri në konsideratë për komunikim vetëm ato nyje të cilat janë të gatshme të marrin pjesë në path_in e rrugëzimit. Kur nyjet e ndërmjetme do të kenë nivele të mirë të baterisë atëherë vetëm destinacioni do të marri mesazhin kërkesë rrugëtim. Pra, mesazhi i parë që arrin në destinacion konsiderohet që do të ndjekë një të energji efikas, si dhe rrugën më të shkurtër të mundshme. Ky protokoll ndihmon për të vlerësuar konsumin e energjisë dhe ekuilibrin në të gjitha nyjet mobile, rezultatet e mara nga simulimit tregojnë se ajo ka arritur konsumin e ekuilibruar të energjisë në të gjitha nyjet me sukses e cila është 35% më shumë se ajo e DSR(Baisakh, April 2013).

Por duhet theksuar se nuk mungojnë situata të tilla kur një nyje e vetme e ndërmjetme e një rruge totale e ka nivelin e energjisë së baterisë më të ulët se vlera e tij e pragut(threshold) (Er <Thr), pra kërkesa për rrugëzim thjesht ndërpritet. Duhet ribërë përsëri kërkesa që rrugëtimi i kësaj nyje të vazhdojë, pra burimi duhet të ridërgojë të njëjtën rrugë por me një numër sekuencial të rritur. Pra ky protokoll mund të përmirësoj dhe të ketë më shumë suksesë se protokolli DSR por nuk e zgjidh përfundimisht problemin që lind gjithmonë në konsumin e energjisë së baterisë të nyjes.

- **Protokolle gjeografike të Internetit**

Për disa prej këtyre protokolleve do të flasim gjatë në çështjet e kapitujve në vijim, si për shembull për protokollin AODV, DSDV, FSR, DSR, ABR,etj.. Ndërkohë më poshtë po trajtojmë protokollin NPV:

NPV(Neighbor Position Verification Protocol): Në rrjetet ad hoc mobile, ku një infrastrukturë fixe nuk është e pranishme analizojmë protokolle reaktive të tilla si verifikimi i pozicionit të fqinjit (NPV). Aftësia që të dish vendndodhjen është duke u bërë një aftësi e rëndësishme për pajisje informatike mobile, ku shumë protokolle kanë nevojë për njohuri të pozitës apo pozicionit të nyjeve pjesëmarrëse. Për shembull, njohuritë në lidhje me nyjet fqinje mund të përdoren për rrugëzimin, cluster_im dhe transmetimin në mënyrë efikase. Sa herë që një nyje ka nevojë të dërgojë të dhëna në një tjetër nyje në një rrjet, ajo duhet së pari të di se ku ta dërgojë atë. Nëse nyja nuk mund të lidhet direkt me nyjen e destinacionit, ajo duhet ta dërgojë atë nëpërmjet nyjeve të tjera përgjatë një rruge të duhur deri te nyja destinacion. Në raste të tilla është e domosdoshme që të sigurojë disponueshmërinë e informacionit të fqinjit. Procedura e përshkruar të NPV që mundëson secila nyje për të arritur lokacionet e shpallura nga fqinjët e saj, dhe të vlerësojë vërtetësinë/besueshmërinë e tyre. Por pengesa kryesore është përdorur për të verifikuar pozicionin e fqinjëve që nyjet deklarojnë.

Protokolli NPV është përdorur për shkëmbimin e mesazheve dhe verifikon pozicionin e komunikimit të nyjave. Në këtë protokoll shkëmbehen katër grupe të mesazheve. Ato janë:

- POLL(VOTO) mesazh: Një verifikues S inicion këtë mesazh(VOTO). Ky mesazh është anonim. Identiteti i verifikuar mbahet i fshehur.
- REPLAY(PËRGJIGJE) mesazh: Një fqinj i komunikimit X duke marrë mesazhin e sondazhit do të transmetojë mesazhin PËRGJIGJE pas një intervali kohor.

- REVEAL (ZBULO) mesazh: Mesazhi ZBULO i transmetimit është bërë duke përdorur adresën e vërtetë të verifikuesit MAC. Ajo përmban një dëshmi se S është autori i POLL_it origjinal dhe verifikues i identitetit.
- REPORT(RAPORTI)mesazh: RAPORTI mban pozicionin e X-it, kohën e transmetimit të PËRGJIGJES së X-it, si dhe listën e çifteve të kohëve të pritjes dhe identifikuesit e përkohshëm referuar transmetimeve PËRGJIGJE të marra të X.

Nga hulumtimet e bëra mbi protokollin NPV theksohet se verifikimi i pozicionit fqinj studiohet në kontekstin e rrjeteve ad hoc dhe sensor; Megjithatë, skemat ekzistuese të NPV shpesh mbështeten në nyje të besueshme fixe ose të lëvizshme, të cilat supozohet të jenë gjithmonë në dispozicion për verifikimin e pozicioneve/pozitave të shpallura nga palët e treta. Në mjediset ad hoc, megjithatë, prania depërtuese e secilës infrastrukturë apo nyjeje fqinje që mund ti besohet apriori është mjaft jorealiste.

- **Protokolle që lidhen me sigurinë dhe menaxhimin**

Standardi IEEE 802.10 ofron specifikimet për një protokoll të sigurisë të shtresës së ndërvepruese të të dhënave dhe shërbimet e ndërlidhura me sigurinë. Protokolli i shkëmbimit të sigurt të të dhënave (SDE-Security Data Exchange) është i mbështetur nga një protokoll i menaxhimit kryesor/kyç të shtresës së aplikimit (KMP) që përcakton asociacione të sigurisë për SDE dhe protokollet e tjera të sigurisë. Një opsion i etiketuar i sigurisë është i specifikuar që të mundësojë kontrollin e aksesit bazuar në rregulla që do të zbatohen duke përdorur protokollin SDE. Pra IEEE 802.10 është një standard i vjetër/mëparshëm për funksionet e sigurisë që mund të përdoren në të dy rrjetet LAN dhe MAN të bazuara në protokollet IEEE 802. 802.10 përcakton menaxhimin e sigurisë dhe menaxhimit kryesor, si dhe kontrollin e aksesit, konfidencialitetin dhe integritetin e të dhënave.

IEEE 802,11 është një grup i MAC(media access control) dhe i specifikimeve të shtresës fizike (PHY) për implementimin e komunikimit kompjuterik të rrjetit lokal wireless (WLAN) në 900 MHz dhe 2.4, 3.6, 5, dhe me banda të frekuencave 60GHz. Ato janë krijuar

dhe mirëmbahen nga Instituti i Inxhinierëve Elektronikë dhe Elektrike (IEEE), Komiteti i Standardeve (IEEE 802) LAN / MAN .

IEEE 802,11 është aktualisht standarti më i përdorur gjerësisht i rrjetit lokal wireless në botë. Për shkak të përdorimit të saj të gjerë, çmimi i kësaj pajisje me performancë relativisht të lartë është shumë i ulët, duke e bërë atë hardware_in më të zgjedhur për testbeds IVC. 802,11 Shtresa e MAC zbatohet praktikisht në të gjithë simulatorët e rrjetit, duke bërë vlerësimin e performancës së sistemeve të IVC bazuar në 802.11 hardware relativisht të lehtë.

Ka disa specifikime standartesh në familjen 802,11: 802.11a; 802.11b; 802.11e; 802.11g ; 802.11n ; 802.11ac Wave 2**;** 802.11ad **;** 802.11ah**;** 802.11r; 802.1X. Secili prej standarteve është një specifik i tipit wireless që operon në banda të ndryshme, të përcaktuara frekuencash.

P.sh 802.11e; është një draft standard wireless që përcakton mbështetjen e cilësisë së shërbimit (QoS) për LAN, dhe është një përmirësim/shtim për specifikimet wireless LAN (WLAN) të 802.11a dhe 802.11b. 802.11e shton karakteristikat e QoS dhe mbështetjen multimediale për standardet wireless ekzistues IEEE 802.11a dhe IEEE 802.11b, duke ruajtur pajtueshmërinë e plotë me këto standarde.

- **Protokolle që lidhen me kontrollin e trafikut**

HRMA(Hop Reservation Multiple Access)- Një protokoll MAC shumëkanalësh i ri për rrejtat packet-radio i bazuar në spektër përhapje i kapërcim - frekuencave shumë të ngadalta. HRMA e lejon një çift të nyjeve komunikuese të rezervoj një kanal duke përdorur një rezervim - hop dhe mekanizëm shtrëngues në çdo hop për të garantuar transmetimin e të dhënave pa-përplasje në prani të terminaleve të fshehura. HRMA siguron një bazament për të ofruar QoS në rrjetet ad-hoc bazuar në radio e thjeshtë të ngadaltë gjysmë-duplex FHSS. Pra siç mund të vërehet protokolli HRMA në ndryshim nga protokolli MAC arrin të realizojë nëpërmjet mekanizmit të përdorur(siç tekoshet më lartë) transmetimin e të dhënave pa përplasje, por deri në çfarë mase mund ta arijë këtë? Dhe gjithmonë problem ngelet bandwidth i përdorur dhe fuqia e baterisë në nyjet, operacioni i shpërndarjes dhe sinkronizimit, etj..

1.4.2 Konkluzione

Pavarësisht nga metodat, sistemet dhe shërbimet e Navigimit të përdorura nga Marina deri më sot probleme të rëndësishme shfaqen në komunikimet ndër- navale të emergjencës. Këto probleme nuk shfaqen vetëm tek nevoja për bandwidth por edhe tek siguria në shërbime dhe sistemet e përdorura, tek shkëputjet në komunikimet anije me breg dhe anije me anije. Këto problem i shohim të shfaqen qoftë tek sistemet Satelitore ashtu edhe tek rrjetat celulare. Por jo vetëm, edhe tek protokollet që ne përmendëm më lartë u vu re se ka nevojë për përmirësim dhe rregullim të transmetimit të paketave të të dhënave nga nyja në nyjë, rritje të informacionit të sigurtë për nyjen fqinje, minimizimin e konsumit të energjisë totale të transmetimit për komunikime multi-hop, zgjedhjen e një rrugë me fuqi më minimale të transmetimit, por jo me shumë Hop_e, dhe rrjedhimisht të gjitha këto ndikojnë në komunikimin mjet me mjet.

GAO(Government Accountability Office) në kërkimet e saj së fundmi zbuloi se në sistemet e komunikimit mungon besueshmëria e nevojshme, shpejtësia dhe bandwidth_i. Dhe ndërtimi i një infrasrukture për këto lloje komunikimesh rezulton shumë i shtrenjtë. Sipas saj Marina nuk e ka trajtuar plotësisht pamjaftueshmërinë për të trajtuar të dhënat e rrjedhshme të vazhdueshme të nevojshme LCS të një sistemit të madh.

Edhe në trajtimin që iu bë protokolleve të rutimit të përdorura në komunikimet ndërmjetor/internavale u vërejt që këto protokolle përdornin përmbytjen (flooding) i cili performon relativisht mirë për një numër të kufizuar të nyjeve, por kjo performancë bie ndjeshëm nëse numri i nyjeve rritet. Kur secila nyje merr dhe transmeton mesazhin pothuajse në të njëjtën kohë, kjo shkakton konflikt dhe përplasje, probleme në transmetim dhe konsumim të lartë të bandwidth_it.

Prandaj, një algoritëm i mirë rutimi mund të shmang bllokimin e trafikut mbi të gjitha linjat. Dhe sfida e të gjitha protokolleve adreson në drejtim të shkallëzimit (scalability) dhe efektivitetit, dhe ky është edhe synimi ynë në këtë punim kërkimor shkencor. Synim ky që do të mundohemi ta përmbushim duke përdorur një protokoll të ri rutimi, ***protokollin tonë InterNavComm.***

KAPITULLI II: AD-HOC KOMUNIKIMI I SIGURT

2.1 Hyrje. Një vështrim i përgjithshëm mbi dy tipet e rrjeteve ad-hoc wireless, MANETs dhe VANETs.

Nëse i referohemi objektit të studimit që u theksua në hyrje, në komunikimin anije me anije komunikimi i lëvizshëm ad-hoc është i përshtatshëm pasi ai ofron pathet e komunikimit alternative për infrastrukturat e komunikimit pa nevojën e mbulimit nga stacionet bazë. Protokolle të ndryshme rutimi janë zhvilluar për rrjetet ad-hoc wireless.

Ashtu siç e dimë tashmë, rrjetat ad-hoc janë rrjeta spontane, të krijuara nga nyje spontane në mjedise me ose pa mbulim të rrjetit të zakonshëm celular. Këtij përkufizimi i përshtaten dhe grupimet e anijeve në porte ose pranë tyre. Për këtë arsye në këtë punim komunikimi ndërmjet anijeve do të modelohet si një komunikim ndërmjet nyjeve të rrjetit ad-hoc, si një komunikim i shpejtë, efiçent dhe i sigurtë.

Rrjeti ad hoc wireless:

- ✓ është rrjeti pa stacione bazë "pa-Infrastrukturë "ose multi-hop
- ✓ një koleksion i dy ose më shumë pajisjeve të pajisur me komunikim pa-tel dhe aftësinë e rrjeteve
- ✓ mbështet në çdo kohë dhe kudo informatikën
- ✓ dy topologji:
  - heterogjene (majtas)
    - dallimet në aftësitë
  - homogjene ose plotësisht simetrike (Djathtas)
    - të gjitha nyjet i kanë njëjta aftësitë dhe përgjegjësitë

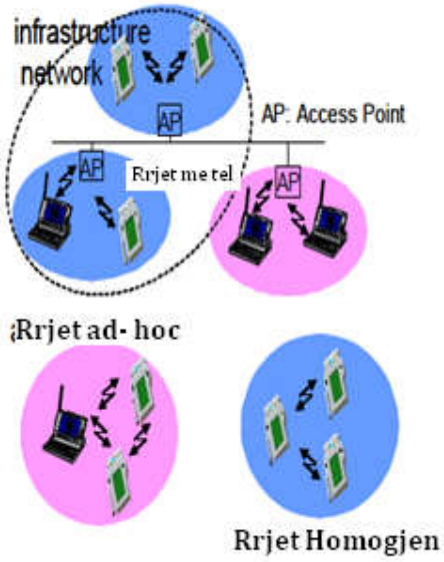


Figura 2.1 Infrastruktura e rrjetit ad hoc

Të kuptosh dhe paraqitësh këtë lloj të ri rrjetash është një sfidë sa e bukur po aq dhe e vështirë. Një karakteristikë kryesore është nevoja për të kuptuar çështje nga shumë fusha të ndryshme, duke filluar nga aspekte të nivelit të ulët të hardware dhe komunikimit radio te konceptet e nivelit të lartë si bazat e të dhënave apo dhe të vetë aplikacioneve të shumta.

Prandaj si fillim në këtë kapitull do të trajtojmë, karakteristikat e dy tipve të rrjeteve ad-hoc wireless, MANETs dhe VANETs, arkitekturën e rrjetave ad-hoc wireles për të kuptuar aspektin hardware te tyre, më pas komunikimin pikë me pikë dhe sigurinë si një pikë e fortë e rrjeteteve ad-hoc wireless, sfidat si dhe fushat e aplikimit për këto lloje rrjetesh.

2.1.1 MANETs

Rrjetat Ad-hoc janë fasilitatorët më të rëndësishëm të komunikimit të brezit të ardhshëm. Rrjete të tilla mund të formohen dhe të konfigurohen në mënyrë dinamike dhe ato mund të jenë të lëvizshme, të pavarur ose të ndërlidhura me rrjetet e tjera. Rrjetat Mobile Ad-hoc (MANETs) janë themeluar nga një grup i nyjeve autonome që të komunikojnë me njëri-tjetrin duke krijuar një rrjet radio multihop dhe për të ruajtur lidhjen në mënyrën pa infrastrukturë. Në rrjetin ad hoc lidhja/setup i rrugës ndërmjet nyjeve përfundon përmes nyjes së ndërmjetme të lëvizshme. Rrjeti wireless mesh dhe rrjeti wireless sensor janë shembulli i rrjetit ad hoc. Rrugëzimi dhe menaxhimi i burimeve bëhet në mënyrë të shpërndarë, teknika 'packet switching'[18] është përdorur për komunikim. Ad hoc është një rrjet efektive i kushtueshëm dhe shumë e vështirë për të arritur sinkronizimin në kohë dhe konsumin e bandwidth.

MANET mori sukses të veçantë, si dhe vëmendje të madhe për shkak karakteristikave apo sjelljeve së tij të vetëmirëmbajtjes dhe vetëkonfigurimit. Në fazat e tij të hershme së shumti njerëzit u fokusuan në mjedisin e tij miqësore dhe bashkëpunues dhe për shkak të kësaj mënyrë shumë probleme të ndryshme erdhi në ekzistencë. Po kështu protokollet e rutimit MANET në thelb kanë besimin se të gjithë pjesëmarrësit duhet të jenë bashkëpunues nga natyra dhe ata varen nga nyjet fqinje për drejtimin e paketave deri në destinacion. Megjithë përparësitë e tij, një model i tillë u lejon hapësirë nyjeve keqëdashëse të cilat mund të dëmtojnë potencialisht lidhjet e komunikimit në MANET ose zbulojnë të dhëna

[18] Lëvizja e paketave

konfidenciale duke nisur lloje të ndryshme sulmesh. Prandaj siguria e lidhjeve ndërmjet pajisjeve dhe rrjeteve është vendimtare dhe një nga shqetësimet kryesore për të siguruar komunikim të sigurt ndërmjet nyjeve të ndryshme në një mjedis të MANET. Propozimi i mekanizmave të duhur të sigurisë është një nga objektivat kryesore për komunikimet MANET.

Rrjeti Mobile ad hoc ka sfida të ndryshme në lidhje me sigurinë wireless për shkak të disa nga arsyet e mëposhtme:

1. Rrjeti wireless përgjegjës në veçanti për sulmet për shkak të përgjimit aktiv në ndërhyrjet pasive.
2. Për shkak të mungesës që shton Pala e Tretë e Besuar, është shumë e vështirë vendosja ose zbatimi i mekanizmave të sigurisë.
3. Pajisjet kryesisht celularë kanë të kufizuar aftësinë llogaritëse dhe funksionalitetet e konsumit të fuqisë të cilat janë më të prekshme ndaj Sulmeve të Mohimit të Shërbimit (Denial of Service attacks). Ai gjithashtu nuk është në gjendje të ekzekutojë algoritme te fuqishme të sigurisë që nevojitin llogaritje të larta si algoritma çelës publik.
4. Për shkak të karakteristikave të MANET-së si pa infrastrukturë dhe vetë-organizimi, ka më shumë shanse për nyjet e besuara që të rrezikohen/ kompromentohen dhe të nisë sulmi mbi rrjetet. Me fjalë të tjera ne kemi nevojë për t'i mbuluar nga të dy sulmet e brendshëm dhe të jashtëm MANET, ndër të cilat sulmet e brendshme janë më të vështirë për t'u trajtuar.
5. Është e vështirë për të dalluar ndërmjet informacionit kurs të vjetëruar dhe atij të falsifikuar për shkak të mekanizmit të lëvizshmërisë nyjes. Në mekanizmin e lëvizshmërisë nyjes ai zbaton rikonfigurimin e shpesht të rrjetit gjë që krijon më shumë shanse për sulme.

Ka llojeve të ndryshme të sfidave në rrjetin e lëvizshmëm ad hoc të cilat janë dhënë më poshtë:

- Arkitektura e rrjetit të hapur
- Mediume të përbashkët wireless

- Kufizimet të rrepta burimeve
- Topologji rrjeti shumë dinamike

Është gjithashtu e vërtetë se zgjidhjet për rrjetet e telëzuar nuk janë të realizueshme për fushat e rrjeteve mobile ad hoc, është gjithashtu e vërtetë se siguria ka qenë prej kohësh një temë aktive kërkimore në rrjetet pa tel; por për shkak të karakteristikave unike të MANET ka shumë sfida për shkak të sjelljes të vetë organizimit të tij. Është e vërtetë se zgjidhjet ekzistuese të sigurisë për rrjetet e telëzuar nuk zbatohen drejtpërdrejt në fushat e MANET. Fusha e aplikimit të rrjetit ad hoc janë kërkimi emergjent, operacionet e shpëtimit dhe informatikë bashkëpunuese. Disa karakteristika të rrjetit ad-hoc jane:

Lëvizshmëria: vendosja e shpejtë në zonat pa infrastrukturë shpesh nënkupton se përdoruesit duhet të eksplorojnë një zonë dhe ndoshta të formojnë ekipe që të koordinojnë ndërmjet tyre për të krijuar një grup pune të posaçëm/task force ose një mision. Në fakt në këtë rast mund të kemi lëvizshmërinë individuale të rastit, lëvizshmërinë grup, lëvizje përgjatë rrugëve të planifikuara që më parë, etj. Modeli i lëvizshmërisë mund të ketë ndikim të madh në zgjedhjen e një skeme kursi/rrugëzimi dhe në këtë mënyrë ndikon në performancën.

Multi-Hopping[19]*:* një rrjet multi-hop është një rrjet ku rruga nga burimi në destinacion përshkon disa nyje të tjera. Rrjetet ad hoc shpesh paraqesin hops[20] të shumta për negociatat pengesë, ripërdorimin e spektrit dhe ruajtjen e energjisë. Operacionet 'Fushë_beteje' të fshehta gjithashtu favorizojnë një sekuencë të shkurtër hop_esh për të reduktuar zbulimin nga armiku.

Vetë-organizimi: rrjeti ad hoc duhet që në mënyrë të pavarur të përcaktojë parametrat e konfigurimit, duke përfshirë: adresimin, rrugëzimin, grupimin, identifikimin e pozicionit, kontrollin e energjisë, etj. Në disa raste, nyje të veçanta (p.sh., nyjet e lëvizshme të strukturës kryesore) mund të koordinojnë lëvizjen e tyre dhe shpërndarjen në hapsirën gjeografike për të siguruar mbulimin e 'ishujve' të shkëputur/shkyçur.

Ruajtja e energjisë: Pjesa më e madhe e nyjeve ad hoc (p.sh., laptopë, PDAs, sensorë, etj) kanë kufizime në furnizimin me energji elektrike dhe nuk kanë aftësinë për të gjeneruar

[19] Shumë hope/kapercimesh
[20] Hope

energjinë e tyre (p.sh., si panelet diellore). Dizenjimi i një protokolli efikas për energjinë (p.sh., MAC, rrugëzimi, zbulimi i burimeve, etj) është kritike për jetëgjatësinë e misionit.

*Shkallëzueshmëria: N*ë disa aplikacione (p.sh., struktura sensore mjedisore të mëdha, dislokimin në fushëbetejë, rrjetet urbane të automjeteve, etj) rrjeti ad- hoc mund të rritet deri në disa mijëra nyje. Për rrjetet e "infrastrukturës" wireless shkallëzueshmëria menaxhohet thjesht me një ndërtim hierarkik. Lëvizshmëria e kufizuar e rrjetet infrastrukturore mund të trajtohet lehtë duke përdorur IP Mobile ose teknikat lokale handoff[21] . Në të kundërt, për shkak të lëvizshmërisë më të gjerë dhe mungesës së referencave fikse, rrjetet e pastër ad hoc nuk tolerojnë IP celular apo një strukturë të hierarkisë fikse. Kështu, lëvizshmëria, së bashku me shkallëzueshmërinë është një nga sfidat më të rëndësishme në hartimin e ad hoc.

Sigurimi: sfidat e sigurisë tek rrjetet wireless tashmë janë të njohura mirë - aftësia e ndërhyrësve për të përgjuar dhe bllokimi i kanalit. Një punë e madhe që është bërë në rrjetet e përgjithshme infrastrukturore wireless shtrihet në domenin ad hoc. Rrjetet ad hoc, megjithatë, janë edhe më të prekshëm ndaj sulmeve se sa homologët infrastrukturore të tyre. Të dy sulme aktive dhe pasive janë të mundshme. P.sh një sulmues aktiv tenton që të ndërpresë operacionet (të themi, një mashtrues duke u paraqitur si një nyje legjitime përgjon/kap kontrollin dhe paketat e të dhënave; riparaqet paketat false të kontrollit; dëmton tabelat e rutimit gjatë riparimit; vendos(në një farë sensi) mohimin e sulmeve të shërbimit, etj). Për shkak të kompleksitetit të protokolleve të rrjetit ad hoc këto sulme aktive janë deri tani më të vështirë për tu zbuluar në ad hoc sesa në rrjetet infrastrukturore.

Sulmet pasiv janë të veçantë për rrjetat ad hoc, dhe mund të jenë edhe shumë më të fshehtë se ato aktive. Sulmuesi aktiv është eventualisht i zbuluar dhe fizikisht me aftësi të kufizuara/i eliminuar. Sulmuesi pasiv asnjëherë nuk zbulohet nga rrjeti. Si një "bug"[22], ai është i vendosur në një fushë të sensorit ose në një cep të rrugës/kënd. Ai monitoron të dhënat dhe modelet e trafikut të kontrollit dhe kështu ndërhyn në lëvizjen e ekipeve të

[21] handoff i referohet procesit të transferimit të një telefonatë në vazhdim ose sesion të dhënash nga një kanal lidhur në rrjetin kryesor në një tjetër kanal.

[22]

shpëtimit në një mjedis urban, ripozicionimin e trupave në terren apo evolucionin e një misioni të veçantë. Ky informacion do të kalojë përsëri në selinë e armikut nëpërmjet kanaleve të posaçme të komunikimit (p.sh., satelitëve apo UAVs) me energji të ulët dhe probabilitet të ulët të zbulimit. Mbrojtja nga sulmet pasive kërkon teknika të reja të fuqishme enkriptimi shoqëruar me dizajne të kujdesshëm të protokollit të rrjetit.

Automjete autonome, pa pilot. Disa aplikacione të rrjetit popullor ad hoc kërkojnë komponentët robotik pa pilot. Të gjitha nyje në një rrjet të përgjithshëm janë sigurisht të aftë për krijimin e rrjeteve autonom. Kur mobiliteti autonome është shtuar gjithashtu, paraqiten disa mundësi shumë interesante për të kombinuara krijimin e rrjeteve dhe lëvizjen. Për shembull, pa UAV (Unmanned Airborne Vehicles) mund të bashkëpunojnë në mbajtjen e një baze të madhe, të ndërlidhur të rrjetit ad hoc në ndikimin e pengesave fizike, parregullsive të kanalit dhe 'zhurmës' së armikut. Për më tepër, UAVs mund të ndihmojë të plotësohen kufizimet e performancës "të kërkesës" nga pozicionimi i duhur dhe reflektimi i antenës.

*Lidhja në internet***:** siç u diskutua më parë, ekziston merita në zgjerimin e rrjeteve të infrastrukturës pa tel në mënyrë oportuniste me shtojcat ad hoc. Për shembull, shtrirja e një LAN_i të brendshëm wireless mund të zgjatet sipas nevojës (në garazh, makina e parkuar në rrugë, shtëpi të fqinjit, etj) me routerat portativ. Këto zgjerime oportune janë duke u bërë gjithnjë e më e rëndësishme dhe në fakt janë rruga evoluese më premtuese për aplikimet komerciale.

- **Qëllimet dhe Objektivat**

MANET është një lloj rrjetit multi-hop, pa infrastrukturë dhe më e rëndësishmja është rrjet vetë-organizues. Për shkak të natyrës pa tel dhe të shpërndarë të tij është një sfidë e madhe për disenjatorët e sistemit të sigurisë. Në vitet e fundit problemet e sigurisë në MANETs kanë tërhequr shumë vëmendje; shumica e përpjekjeve të kërkimit janë përqendruar në fusha të veçanta të sigurisë, si sigurimi i protokolleve kurs ose vendosja e infrastrukturës të besuar apo zbulimin e ndërhyrjeve dhe përgjigjegjeve.

Një nga karakteristikat kryesore të MANET's në lidhje me pikën e projektimit të sigurisë është mungesa e mbrojtjes së linjës së qartë. Në rastin e rrjeteve me tel kemi routera të dedikuar; të cilët kryejnë funksionalitetet e rutimit për pajisjet, por në rastin e MANET shqetësimi qëndron tek fakti që secila nyje vepron/sillet si një ruter duke i shtyrë paketat përpara për nyjet e tjera. Është gjithashtu e vërtetë se kanali wireless është në dispozicion për të dy përdoruesit e rrjetit, pra edhe për sulmuesit. Nuk ka rregull të mirëpërcaktuar apo vend ku trafiku nga nyje të ndryshme duhet të monitorohet ose mekanizmat e kontrollit të përqasjes të mund të zbatohen. Në këtë shkak nuk ka ndonjë linjë mbrojtjese që ndan rrjetin e brendshëm nga rrjeti jashtë. Në këtë mënyrë protokollet kurs ekzistuese ad hoc, si DSR (Dinamik Source Routing) dhe AODV (Ad Hoc On Demand Largësia Vector) dhe protokollet wireless MAC, të tilla si 802.11, zakonisht supozohet t'u besohet. Si rezultat i kësaj, një sulmues mund të bëhet ose sillet si një router dhe të prishi operacionet e rrjetit. Ka kryesisht tre shërbime kryesore të sigurisë për MANETs: Autentifikimi, Konfidencialiteti, Integriteti.

- Autentifikimi nënkupton: identiteti i saktë është i njohur për autoritetin e komunikimit.
- Konfidencialiteti nënkupton: informacioni mesazh mbahet i sigurte nga aksesi i paautorizuar.
- Integriteti do të thotë mesazhi është i pandryshuar gjatë komunikimit ndërmjet dy partive.

Nga të tria këto shërbime të sigurisë, Autentifikimi është ndoshta çështja më e rëndësishme dhe më komplekse në MANETs sepse është ributimi i të gjithë sistemit të sigurisë. Pasi autentifikimi është arritur në MANET atëherë konfidencialiteti është vetëm një çështje e algoritmit të enkriptimit duke përdorur çelësat. Këto shërbime të sigurisë mund të ofrohen në formë individuale apo të kombinuara, kjo varet vetëm nga kërkesat tona.

Ka disa karakteristika të zgjidhjeve të sigurisë të MANETs të cilat do të sigurojnë në mënyrë të qartë zgjidhje të shumta sigurie përsa i përket mbrojtjes së rrjetit dhe gjithashtu të sigurojnë performancën e dëshirueshme të rrjetit:

1. Zgjidhja e sigurisë duhet gjithashtu të implementohet ndërmjet shumë komponenteve individuale për të siguruar mbrojtje kolektive e në këtë mënyrë të sigurojë të gjithë rrjetin. Në kushtet e aftësive llogaritëse/procesuese janë shqetësuese si furnizimi me

energji, memoria si dhe kapaciteti i komunikimit që secila pajisje ka për të punuar në vetvete.

2. Zgjidhja e sigurisë duhet të ofrojë siguri në lidhje me shtresa të ndryshme të pirgut/stakut të protokollit dhe çdo shtresë të sigurojë vijën e mbrojtjes. Është gjithashtu e mundur që vetëm një zgjidhje e një shtrese të vetme mund të trajtojë të gjitha sulmet e mundshme.
3. Zgjidhjet e sigurisë duhet të shmangin të dy tipet e kërcënimeve, të jashtëm, si dhe të brendshëm. Përsa u përket sulmeve të jashtme shqetësimi qëndron në shmangien e sulmeve mbi kanalin wireless, si dhe mbi topologjinë e rrjetit, ku ashtu si në rastin e sulmeve të brendshme një njeri i infiltrues hyn në rrjet me anë të pajisjeve të kompromet uara për të fituar akses mbi njohuri të ndryshme të rrjetit.
4. Zgjidhjet e sigurisë duhet të zbatojnë të tri komponentët e sigurisë si parandalimin, zbulimin, dhe reagim.
5. Zgjidhjet e sigurisë duhet të jenë të përballueshme, si dhe praktike në burime të kufizuara dhe skenar tejet dinamik të rrjeteve.

- **Aplikimet dhe Integrimet e MANET**

Në vijim ne kategorizojmë aplikimet kryesore të MANET:

1. Rrjetet Mesh wireless: këto rrjete mund të sigurojë njëkohësisht lidhje wireless të brendshme dhe të jashtme të broadband në mjedise urbane, periferike dhe rurale pa patur nevojë për infrastrukturë të kushtueshme të rrjetit me tel. Shembuj të rrjeteve të tilla mund të jenë në vijim:
   - rrjetet e aksesit publik të Internetit: Këto janë rrjetet Mesh wireless që mund të ofrojnë broadband, për shembull, në një qytet;
   - sistemet inteligjente të transportit: rrjetet mesh wireless mund të veprojnë si sisteme të shpërndarjes së informacionit për të kontrolluar shërbimet e transportit;
   - Sistemet e sigurisë publike: Rrjetet mesh Wireless mund të jenë mjeti për të adresuar kërkesat e agjencive të zbatimit të ligjit dhe qeverive të qytetit duke

mbështetur komunikimet ushtarake apo komunikimet emergjente si zëvendësim i sistemeve aktuale të PPDR (Public Protection Disaster Relief)

2. Rrjetet oportune: këto rrjete mund të sigurojnë lidhje të përhershme në internet në zonat rurale dhe ato në zhvillim në çmime të ulëta. Një tjetër kërkesë i rrjetave oportune mund të jetë, për shembull, monitorimi i kafshëve të egra për të gjetur speciet e egra, të shqyrtojë sjelljen e tyre dhe për të kuptuar reagimin e tyre ndaj ndryshimeve të ekosistemit për shkak të veprimtarive njerëzore.
    - Rrjetet ad-hoc të automjeteve: këto rrjete përdorin komunikimet ad-hoc për të ndihmuar drejtimin dhe rritjen e sigurisë së makinës. Shembuj të këtyre komunikimeve mund të jetë përhapja e të dhënave nga anët e rrugës dhe nga makina të tjera ose ofrimi i informatave të lidhur me pengesat gjatë rrugës, ngjarjet emergjente dhe informacione të trafikut për shoferët (që kërkojnë multi-hopping, kryesisht për shkak të kufizimit të linjës-shikimit).
3. Rrjetet Sensor Wireles: këto rrjete përbëhen nga sensorë wireless që fuqizojnë baterinë me aftësitë llogaritëse dhe komunikuese. Shembuj të aplikimeve të rrjeteve sensor wireless që synojnë të komunikojnë informacionin ndërmjet sensorëve apo te një entitet qendror, mund të jenë si më poshtë:
    - Aplikacionet e gjurmimit: nyjet sensore mund të vendosen që të ndjejnë praninë e personave dhe objekteve në zona të caktuara;
    - Shtëpitë e zgjuara: në shtëpitë e sotme sensorët wireless dhe aktivizuesit mund të komunikojnë me mjedisin dhe njerëzit, ofrimit të shërbimeve të brezit të ardhshëm si matje e zgjuar, ndriçimi i zgjuar e kështu me radhë;
    - Monitorimi mjedisor: sensorët wireless mund të përdoren për zbulimin e zjarrit pyjor, zbulimin e përmbytjeve, për të lejuar një reagim të shpejtë përpara se një aksident të bëhet i pakontrollueshëm;
    - Monitorimi i shëndetit: sensorë pa tel mund të përdoren si pjesë e një sistemi të monitorimit të shëndetit të ofruar për një pacient. Sensorë të tilla mundet, për shembull, të komunikojnë me mjekun e pacientit për të dërguar njoftime në lidhje me gjendjen shëndetësore apo alarme në rast të një gjendje shëndetësore emergjente.

2.1.2 VANET s

Përparimet e fundit në teknologjitë wireless kanë mundësuar komunikimet ndërmjet automjeteve (IVC(Inter- Vehicular Communications)) në rrjetet mobile ad hoc (MANETs) dhe kjo ka çuar në lindjen e një lloj të ri të MANET njohur si VANETs.

Pra Vehicular Ad hoc Networks (VANET) është pjesë e Mobile Ad Hoc Networks (MANETs), kjo do të thotë se çdo nyje mund të lëvizi lirisht brenda mbulimit të rrjetit dhe të qëndrojë e lidhur me të tjera nyje, çdo nyje mund të komunikojë me nyjet e tjera në një hop të vetëm ose multihop, dhe çdo nyjë mund të jetë vet mjeti, RSU (Road Side Unit). Sistemi i rrjetizimit të automjeteve konsiston në një numër të madh nyjesh, numri i automjeteve zë një shifër shumë të madhe, këto mjete do të kërkojnë një autoritet për ta qeverisur atë, çdo automjet mund të komunikojë me automjete të tjera duke përdorur sinjale të shkurtër radio. Në fakt VANETs kanë teknologji ndërfaqe radio të ngjashme ose të ndryshme, duke punësuar me rreze të shkurtër në sistemet e komunikimit me rreze të mesme. Gama radio e VANETs është disa qindra metra, zakonisht ndërmjet 250 dhe 300 metra. Në SHBA, Komisioni Federal i Komunikimit (FCC) ka ndarë 75 MHz në brezin 5.9 GHz për të licencuar DSRC(Dedicated Short Range Communication) për automjet-me-automjet dhe automjete me komunikim me infrastrukturë. Ky komunikim është një komunikim Ad Hoc që do të thotë se çdo nyje e lidhur mund të lëvizi lirshëm, nuk kërkohen tela, ruterat përdorin të ashtëquajturat RSU (Road Side Unit), RSU punon si një ruter ndërmjet automjeteve në rrugë dhe pajisjeve të tjera të rrjetit. (K.Prasanth, Dr.K.Duraiswamy, K.Jayasudha, and Dr.C.Chandrasekar March 2010)

Siç mund ta dimë nga sondazhet dhe evidencat, miliarda njerëz në mbarë botën vdesin çdo vit në aksidente me makinë dhe shumë të tjerë plagosen. Implementimi i informacioneve të sigurisë të tilla si kufijtë e shpejtësisë dhe kushtet e rrugës janë përdorur në shumë pjesë të botës, por ende shumë punë është e nevojshme në këtë drjetim. VANET duhet, në zbatimin, mbledhjen dhe shpërndarjen e informacionit të sigurisë të reduktojë masivisht numrin e aksidenteve duke paralajmëruar shoferët në lidhje me rrezikun para se ata në fakt të përballen me atë. Rrjete të tilla përbëhen nga sensorët dhe Obu (On Board Units) të instaluar në makinë, si dhe RSU_të.

Megjithëse aplikimet e sigurisë janë të rëndësishme për qeveritë që të ndajnë frekuenca për komunikime automjetesh, aplikacione jo të sigurisë janë po aq të rëndësishme për Sistemet Inteligjente të Transportit (ITS) për tri arsye:

1. Sistemet ITS mbështeten në pajisje thelbësore të cilat duhet të instalohen në çdo makinë dhe është gjerësisht i disponueshëm për përdoruesit. Megjithatë, ka pak gjasa që individët të mund të përballojnë këto pajisje të shtrenjta.
2. Aplikacionet e sigurisë në përgjithësi kërkojnë bandwidth të kufizuar për intervale të shkurtra kohore. Meqë efikasiteti i bandwidth është një faktor i rëndësishëm, aplikacione jo të sigurisë janë të rëndësishme për të rritur efikasitetin e bandwidth.
3. Disponimi i RSU ofron një infrastrukturë që mund të përdoret për të siguruar mjaft shërbime me vetëm një rritje të vogël në kosto.

Teknologjia VANET integron rrjetin ad hoc, WLAN (LAN wireless) dhe teknologjinë celulare për të arritur IVC(Inter-Vehicle Communications) inteligjente dhe RVC (Roadside-to-Vehicle Communications). (K.Prasanth, Dr.K.Duraiswamy, K.Jayasudha, and Dr.C.Chandrasekar March 2010)

Shpejtësitë e mjeteve janë gjithashtu të kufizuara në përputhje me kufijtë e shpejtësisë, nivelin e dyndjes në rrugë, dhe mekanizmave të kontrollit të trafikut. Përveç kësaj, duke pasur parasysh faktin se automjetet e ardhshme mund të jenë të pajisur me mjete me rangje transmetimi potencialisht të gjata, burime të ringarkueshëm të energjisë, dhe kapacitete magazinimi ekstensive në bord, përpunimi energjisë dhe efikasiteti i magazinimit nuk janë një problem në VANETs siç janë në MANETs. Nga këto karakteristika, VANETs janë konsideruar si model rrjeti jashtëzakonisht fleksibël dhe relativisht "lehtësisht të menaxhueshëm" të MANETs. Për shkak të zhvillimeve të fundit në fushën e VANET, një numër i aplikacionesh tërheqëse, të cilat janë unike për vendosjen e veprimin e tyre në automjete, kanë dalë.

Garantimi i një mekanizmi kurs të qëndrueshëm dhe të besueshëm për VANETs është një hap i rëndësishëm në drejtim të realizimit të komunikimeve efektive të automjeve. Protokollet ekzistues kurs, të cilat janë projektuar tradicionalisht për Manet, nuk përdorin karakteristika unike të VANETs dhe nuk janë të përshtatshme për komunikimet automjeti-

me-automjet për VANETs. Në të vërtetë, mesazhet e kontrollit në protokollet reaktive dhe kohëmatësit e përditësimit të kursit në protokollet proaktive nuk janë përdorur që të parashikojnë thyerjen e link_ut. Ata vetëm tregojnë praninë ose mungesën e një rruge/kursi në një nyje të caktuar. Si pasojë, proçesi i mirëmbajtjes të kursit në të dy llojet e protokolleve fillon vetëm pasi një ngjarje thyerje-link ndodh. Në një sistem tepër dinamik siç është VANET, ku thyerje-linku është i shpeshtë, kërkesa për përmbytje në masë të madhe do të degradojë punën e sistemit për shkak të futjes së trafikut shtesë të rrjetit në sistem dhe ndërprerjes në transmetimin e të dhënave.

- **Karakteristika të VANETs**

Duke krahasuar VANETs me MANETs në vazhdim, më poshtë, do të nxjerrim disa nga karakteristikat kryesore të VANET. (Fan Li and Yu Wang, June 2007)

Fuqia e pakufizuar e transmetimit: Çështjet e fuqisë së pajisjes mobile nuk janë një pengesë e konsiderueshme në rrjetet e automjeteve. Vetë automjeti të mund të sigurojë energji të vazhdueshme për fuqinë dhe pajisjet e komunikimit.

Aftësi të lartë llogaritëse: Automjetet operative mund të përballojnë aftësi të rëndësishme kompjuterike, komunikimi dhe të ndjeshmërisë

Topologjia e lartë dinamike: skenarët e rrjetit të automjetit janë shumë të ndryshme nga rrjetet klasike ad hoc. Në VANETs, automjetet mund të lëvizin shpejt. Kjo tregon se topologjia në VANETs ndryshon shumë më shpesh.

Lëvizshmëria e parashikueshme: Ndryshe celular rrjeteve klasike ad hoc, ku është e vështirë të parashikohet lëvizshmëri e nyjave, automjetet kanë tendencë të kenë lëvizje shumë të parashikueshme që janë (zakonisht) të kufizuara në rrugë. Lëvizja e nyjeve në VANETs kufizohet nga layout i rrugëve. Informacioni rrugor është shpesh në dispozicion nga sistemet e pozicionimit dhe teknologjitë e bazuar në hartë siç është GPS. Çdo çift nyjesh mund të komunikojë drejtpërdrejt, kur ato janë brenda kufijve radio.

***Në shkallë potencialisht më të madhe*:** Ndryshe nga rrjetet ad hoc rrjetet e automjeteve në parim mund të shtrihen mbi të gjithë rrjetin rrugor dhe kështu përfshijnë shumë pjesëmarrës.

Rrjet i particionuar: Rrjetet e automjeteve shpesh particionohen. Natyra dinamike e trafikut mund të rezultojë ose çojë në boshllëqe të mëdha ndër automjete, në skenarët pak të populluar dhe kështu në disa grupe të izoluara të nyjeve.

Lidhja e Rrjetit: Shkalla në të cilën rrjeti është lidhur është shumë e varur nga dy faktorë: Shkalla e linkeve Wireless dhe pjesa e mjeteve pjesëmarrëse, ku vetëm një pjesë e automjeteve në rrugë do të jetë e pajisur me ndërfaqe wireless. (Fan Li and Yu Wang, June 2007).

Siç tregon ky studim, por edhe studime të tjera u bë shumë kohë që hulumtohet rreth rrjeteve ad hoc, por VANET do të formojnë rrjetin më të madh ad hoc të implementuar ndonjëherë, prandaj çështjet e mobilitetit, stabilitetit, besueshmërisë dhe shkallëzueshmërisë janë shqetësuese dhe sfida kryesore të këtyre tipe rrjetash. Le të trajtojmë disa prej këtyre sfidave:

Lëvizshmëria: Ideja themelore prej rrjeteve ad hoc është që çdo nyje në rrjet është e lëvizshme dhe mund të lëvizi nga një vend në tjetrin brenda zonës së mbulimit, por ende mobiliteti është i kufizuar, në rrjetet ad hoc të automjeteve nyjet lëvizin në lëvizshmëri të lartë, automjetet bëjnë lidhje përmes rrugës së tyre me një tjetër automjet që ndoshta nuk e kanë hasur kurrë më parë, dhe kjo lidhje zgjat vetëm disa sekonda pasi çdo automjet shkon në drejtimin e vet, dhe këto dy automjete mund të mos takohen përsëri. Pra, sfida e sigurimit të mobilitetit është problem i vështirë .

Luhatshmëria/paqëndrueshmëria*:* Lidhja ndërmjet nyjeve mund të jetë shumë kalimtare, dhe ndoshta nuk do të ndodhë përsëri, Automjetet udhëtojnë përmes zonës së mbulimit duke kyer lidhjen me automjete të tjera, këto lidhje do të humbin, pasi çdo makinë ka një lëvizshmëri të lartë dhe ndoshta do të udhëtojë në drejtim të kundërt .

Shkallëzueshmëria e rrjeti: Shkalla e këtij rrjeti në botë afërsisht i tejkalon 750 milionë nyje dhe ky numër është në rritje, një problem tjetër lind kur ne duhet të dimë se nuk ka një autoritet globale të qeveris standardet për këtë rrjet, për shembull: standardet për DSRC[23] në Amerikën e Veriut janë të ndryshme nga standardet DSRC në Evropë, standardet për GM Automjetet janë të ndryshme nga ai i BMW.

- **Aplikimet e VANET:**

[23] Dedicated Short Range Communications- teknologji për të zbuluar rreziqet e mundshme në rrugën e një automjeti

Një numër i madh i aplikacioneve janë specifikuar nga qeveritë për aplikimet DSRC, ne të mbulojë këtu disa prej tyre. kontrolli i trafikut është një faktor i madh për përdorim efikas të rrjetit. Aktualisht dritat e trafikut organizojnë rrjedhën e trafikut në kryqëzime. Me DSRC dritat e trafikut bëhen të adaptueshme për trafikun dhe mund të sigurojnë përparësi ndaj mjeteve të urgjencës, si dhe sigurinë për këmbësorët dhe çiklistët. Gjithashtu informacioni rreth gjendjes së rrugës mund t'u shpërndahet automjeteve për t'i paralajmëruar për problemet që vijnë si akulli ose mirëmbajtjet e punës në rrugë. Ky sistem do të jetë shumë efikas në rastin e aksidenteve, automatikisht njoftohet ambulanca me e afërt dhe automjete të tjera të emergjencës t'i afrohen aksidentit nëse është e nevojshme dhe madje edhe të ofrojnë shërbime të telemjekësisë në qoftë se pacienti kërkon vëmendje të menjëhershme, sidomos kur nuk ka spitale aty pranë. parandalimi përplasjes është motivi kryesor pas ITS, prandaj një numër i aplikacioneve janë të specifikuara. Aplikacionet e parandalimit të përplasjes që mbështeten në një infrastrukturë përfshijnë: paralajmërime gjeometrike të rrugës për të ndihmuar shoferët në të pjerrët/dishesë ose në rrugë të lakuara dhe paralajmërime për automjetet me mbipeshë ose me mbi lartësi, sisteme të përplasjes dhe të ndërprerjes me linjat hekurudhore për ti ndihmuar shoferët, këmbësorëve, çiklistët të kalojnë në mënyrë të sigurtë, dhe sisteme paralajmëruese të kafshëve që informojnë drejtuesit mbi përplasje të mundshme, këto sisteme bëhen të një rëndësie jetike natën apo në kushtet e shikimit të ulët. Aplikacionet e sigurisë të cilat nuk mbështeten në një infrastrukturë përfshijnë një njoftim mbi frenat e emergjencës i cili është aplikimi më i rëndësishëm për parandalimin e përplasjes/rrëzimit. Dy makinat e para mund të mos përfitojnë nga sistemi i frenave emergjente, por makinat e mëtejshme mund ta shmangin aksidentin. Ndihma e ndryshimit të korsisë, zbulimi i pengesës rrugore, paralajmërimi për largim nga rruga, si përpara dhe pas përplasjes janë të gjithë shembuj të aplikimeve të sigurisë V2V. Mjetet mund të dërgojnë automatikisht kërkesa ndihme në rast të një aksidenti që mund të jetë me rëndësi jetike kur ka makina të tjera rreth tyre. Një projekt i vazhdueshëm evropian, eCall, ka për qëllim ofrimin e këtij shërbimi automatik të thirrjes që nga 2009 duke përdorur infrastrukturën ekzistuese celulare. Sistemi OBU(On Board Unit) mund të ndihmojë drejtuesin në mënyra të tjera të ndryshme të tilla si zgjerimin e vizionit nëpërmjet teknikave të përpunimit të imazhit, asistencën e mbajtjes së korsisë dhe monitorimin e sistemeve në bord, si dhe ndonjë

ngarkesë apo rimorkio të lidhur me automjetin. Sistemet të tilla janë përgjithësuar si ADAS(Advanced Driver Assistance Systems).

Aplikimet komerciale të sistemit mbulojnë një gamë të gjerë të ideve të reja mbështetëse të individëve dhe turistëve të tilla si rezervimin e një vend parkimi, shkarkimin e informacionit të turizmit dhe harta për restorantet dhe stacionet e furnizimit me gaz, navigacion dhe drejtimin e rrugës, pagesa për sheshet rrugore, akses në Internet dhe lidhje me kompjutera në shtëpi. Pajisje të tjera brenda mjetit mund të jetë të lidhura me OBU(On Board Units) për të hyrë në çdo shërbime të ofruara nga rrjeti, ose nëpërmjet internetit. Këto aplikacione nuk janë të kërkuara nga qeveria, por ata i inkurajojnë njerëzit për ta instaluar sistemin.

Një projekt Japanese i quajtur PDRGS (Dynamic Route Guidance System[24]) është një zbatimi i mundshëm i navigimit dhe i shërbimit rrugor. Ky projekt është duke zhvilluar një sistem të njohur si PRONAVI i cili aktualisht përbëhet nga një server me akses përmes internetit. Përdoruesit fusin pozicionin e fillimit të tyre, destinacioni dhe koha për të filluar udhëtimin e tyre dhe serveri përgjigjet me dy rrugëve më të mira. Rrugët janë hartuar nga një sondazh 9 mujor, si dhe simulimet. Në versionin e tij përfundimtar sistemi duhet të jetë në gjendje të mbledhë të dhëna nga sensorë të instaluar në makina dhe të sigurojë rrugët për në OBU.

Sistemi i komunikmit dhe informimit të mjetit, VICS(The Vehicle Information and Communication System) është një tjetër implementim Japonez i rrugës tek komunikimi i mjeteve. Abonentët tek sistemi marrin një sistem navigacioni nëbord ku marrin informacione rreth motit, kushteve të rrugës, trafikut dhe çdo të dhëne tjetër të lidhur me njësitë anësore të rrugës dhe e tregon atë për përdoruesit. Në Evropë iniciativa e eSafety filloi në prill të vitit 2002. Aktualisht ajo ka 14 grupe pune që punojnë në fushat e analizave të shkakut të aksident, të komunikimit, hartave dixhitale, thirrjet emergjente (eCall), automjetet e detyrës së rëndë, IHM(Interaction Machine Human), teknologjitë e informacionit dhe komunikimit për lëvizshmërinë e pastër, implementimi i hartës rrugore, bashkëpunimi ndërkombëtar , trafiku në kohë reale dhe informacione të udhëtimit(RTTI), hulumtim dhe zhvillim, të sigurisë, i arkitekturave të shërbimit të orientuar dhe i

[24] Sistem udhëzues i rrugës dinamike

komunikimi e ndërgjegjësimit të përdoruesit . Forumi eSafety ka për qëllim të përshpejtojë zhvillimin, vendosjen dhe përdorimin e sistemeve të esafety për të zvogëluar numrin e vdekjeve në Evropë në 50% deri në vitin 2010.

Projekti CARLINK u nis në vitin 2006 nga CELTIC EUREKA me informacion lokal të motit në kohë reale, menaxhimin e trafikut të transportit urban dhe transmetimin e informacionit urban si aplikimet kryesore. Ajo ka për qëllim integrimin e WLAN, WiMAX si dhe teknologjinë celulare për të siguruar informacion për makinat në rrugë, si dhe për PDAs dhe telefonat celularë.

2.2 Arkitektura e Rrjetave Ad-Hoc Wireless

Përveç të gjitha çështjeve të trajtuara më lartë një tjetër çështje apo pikë po kaq e rëndësishme për tu trajtuar është arkitektura e rrjetave ad hoc Wireless. Protokollet e rutimit ad-hoc lejojnë mesazhet që të përcillen përmes nyjeve të shumta sensore duke marrë parasysh ndryshimet dinamike të topologjisë për shkak të, p.sh. mobilitetit të nyjeve apo dhe dështimit të nyjeve. Protokollet e komunikimit duhet të jenë të energjisë-efektive meqë nyjet sensore kanë furnizim të kufizuar të energjisë. Shtresat e shpërndara të shërbimeve përmbajnë shërbime për mbështetjen e aplikacioneve për sensor mobile. Shërbimet e shpërndara koordinojnë me njëri-tjetrin për të kryer llogaritje të decentralizuara dhe modifikime të të dhënave. Mbi këtë tip arkitekture, aplikacionet mund të ndërtohen duke përdorur rrjetin sensor dhe shërbimet e shpërndara.

Arkitektura MANET: Po e fillojmë me arkitekturën e rrjetit mobile Ad-hoc (MANET) që është treguar në figurën 2.2. Arkitektura e këtij rrjeti është grupuar në tre kategori kryesore:

A. Tekonologjitë e mundësuara;
B. Rrjetizimi;
C. Middleware[25] dhe aplikacionet

[25] software kompjuterik i cili vepron si një urë lidhëse ndërmjet një sistemi operativ apo bazë të dhënash dhe aplikacionesh, veçanërisht në një rrjet.

Figura 2.2. Nje arkitekturë e thjeshtë MANET

A. Teknologjitë e mundësuara: Në varësi të zonës së tyre të mbulimit, këto teknologji janë klasifikuar në disa klasa të rrjetave: Personal (PAN), Local(LAN), Metropolitan (MAN) and Wide area(WAN), të cilat janë paraqitur në fig.2.3 më poshtë:

- Një rrjet Body area (BAN), është i lidhur fuqishëm me kompjutera në gjendje të mirë/të përshtatshëm dhe BAN siguron lidhjen midis pajisjeve të tilla si ekranet e montuar, mikrofona, kufje, etj. Rangu i komunikimit të BAN është 1-2 m.
- Rrjeti i hapsirës personale PAN lidhë pajisjet mobile të cilat kryhen nga përdorues të pajisjeve të tjera të lëvizshme dhe të palëvizshme. Rangu i komunikimit të PAN është deri në 10 m.
- Wide(WAN) dhe Metropolitan(MAN) janë rrjete të lëvizshme multi-hop pa tel që përballen me shumë sfida të cilat janë ende për t'u zgjidhur p.sh. adresimi rutimi, menaxhimi i vendodhjes, siguria, etj...

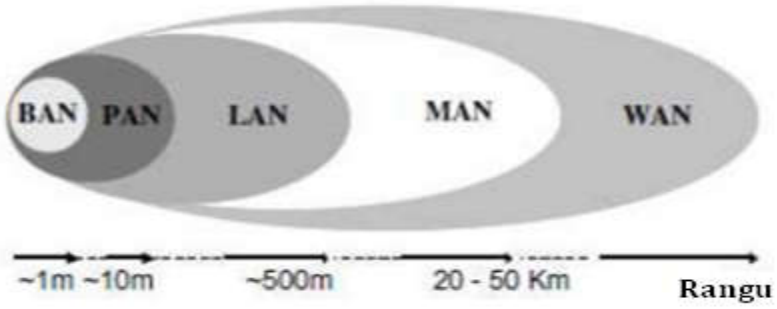


Figura 2.3. Taxonomi e rrjetit ad hoc

B. Në MANET, shumica e funksioneve kryesore të protokolleve të rrjetizimit duhet të jenë ri-dizejnuara për mjedise komunikimidinamikë, vetë- organizues, të paqëndrueshëm, peer-to-peer. Objektivi kryesor i protokolleve të rrjetizimit është që të përdorin shërbimet e transmetimit one-hop të cilat ofrohen nga teknologjitë e mundësuar për të ndërtuar shërbimet të ofrimit (të besueshme) end -to-end, nga një dërgues në një (ose më shumë) marrës/a. Në rast se krijohet një komunikim fund-me-fund; dërguesi ka nevojë për të gjetur marrësin brenda rrjetit. Qëllimi kryesor i një shërbimi lokalizues është që të skicojë dinamikisht adresën logjike të pajisjes (marrësit) për tek vendndodhja korrente/aktuale në rrjet.

C. Middleware dhe Aplikimet. Sidomos në vitet e fundit, me zhvillimin e shpejtë të hulumtimeve në rrjetin mobile,këto rrjete kanë tërhequr interesa dhe vëmendje të konsiderueshme nga industria komerciale e biznesit, si dhe komuniteti i standardeve. Futja e teknologjive të reja, si si WiFi, Bluetooth, IEEE 802,11, WiMAX dhe HyperLAN lehtëson në masë vendosjen e teknologjisë ad hoc, dhe aplikacionet e reja të rrjeteve ad hoc u shfaqën kryesisht në fusha të specializuara të tilla si shërbimet e emergjencës, rimëkëmbje nga fatkeqësit dhe në monitorimin e mjedisit. Sistemet Mobile ad hoc aktualisht të zhvilluara adaptojnë përqasjen e të mos paturit të një middleware, por mbështetin mbi të secilin aplikim për ti trajtuar të gjitha shërbimet që i duhen.

Nyjet e rrjetit mund të operojnë në një nga tre mënyrat që janë projektuar për të lehtësuar reduktimin e fuqisë së përdorur:

- Mënyra/Modaliteti Active: Kjo është mënyra duke përdorur energjinë më të madhe. Kjo i lejon të dyja transmetimin dhe marrjen e mesazheve Doze Mode: CPU është e aftë për përpunimin e informacionit dhe është gjithashtu e aftë për marrjen e njoftimit të mesazheve nga nyjet e tjera.
- Mënyra /Modaliteti Sleep (ose Mode Standby): The CPU nuk kryen procesimin dhe nyja nuk ka aftësinë për të dërguar / marrë mesazhe. Nyja është joaktive. Kjo mënyrë

i lejon një nyje për ta ndaluar "veten" për periudha të shkurtra kohore pa kërkuar energji ose ri-inicializim.

Ekzistojnë dy përqasje për të siguruar lidhjen në rrjet në një MANET:

1. Arkitektura hierarkike e rrjetit: Ky tip arkitekture e ndan të gjithë rrjetin në nën-rrjete. Pastaj, secili prej nën-rrjeteve vetë dinamikisht zgjedh një nyje ndërmjet këtyre nyjeve e cila vepron si portë për nën-rrjetin tjetër. Kjo ndërton një hierarki ndërmjet nyjeve dhe hierarkia mund të jetë një hapsirë/shtresë rrethore ose shumë shtresore. Avantazhet e kësaj arkitekture janë:

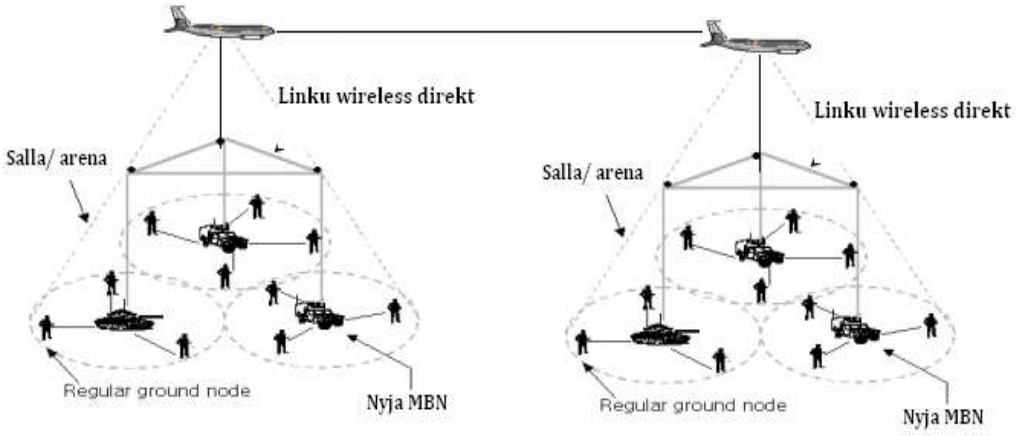


Figura 2.4. Arkitektura hierarkike e MANET

- Procedura të lehtë të menaxhimit të lëvizshmërisë.
- Mundësi menaxhimi më të mira.

Arkitektura hierarkike lind si përgjigje vertikale ndaj problemeve të shkallëzueshmërisë të paraqitura në arkitekturën e sheshtë. Kjo lloj arkitekture rrit kapacitetin e rrjetit duke përmirësuar cilësinë e komunikimit, rutimit dhe kontrollit të topologjisë dhe është një alternativë e mirë për të arritur shkallëzueshmërinë në rrjetet ad hoc

2. Arkitektura e sheshtë(Flat): Në këtë përqasje të gjitha nyjet janë identike në aspektin e përgjegjësisë, dhe nuk ka konceptin e portave të veçanta. Përparësitë e kësaj metode janë:
    - Rritja e besueshmërisë / mbijetesën për shkak të asnjë pikë të vetme të dështimit dhe të rrugëve alternative në rrjet.
    - Rutim optimal
    - Zvogëlimi i përdorimit të burimeve wireless.
    - Vet balancim më i mirë i Ngarkesa
    - Të gjitha nyjet kanë një lloj të pajisjeve

    Në një arkitekturë të sheshtë të gjitha nyjet kryejnë rutimin dhe përcjelljellin paketa në mënyrë të pavarur dhe pa ndonjë kontroll të jashtëm. Në figurën 2.5 është e mundur të vëzhgohet një rrjet ad hoc me një arkitekturë të sheshtë, ku duket qartë se është e nevojshme që të përdoren nyje të ndërmjetme për të arritur komunikimin.

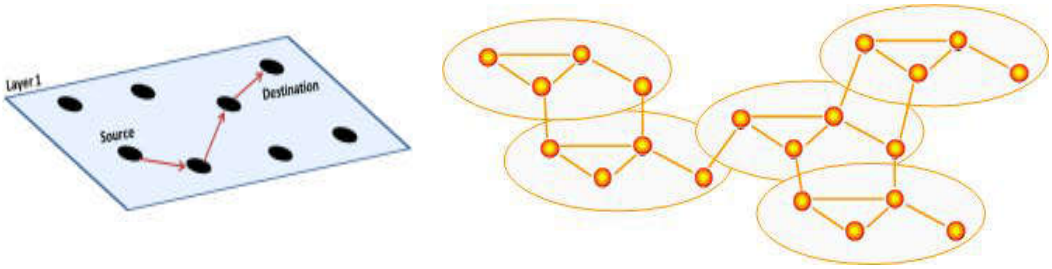


Figura 2.5.Arkitektura Flat

Arkitektura e VANET: Po e nisim me një figurën më poshtë(të paraqitur nga **Fan** Li and Yu Wang, Qershor 2007) e cila paraqet arkitekturat e VANET(për të cilin kemi folur më lartë): Ashtu siç duket qartë edhe në Figurën 2.1, në rastin a) kemi një kominikim mjet me infrastukturë (Vehicular to Infrastructure) V2I; në rastin b) mjet me mjet (Vehicular to Vehicular) V2V dhe në rastin c) Hybrid i V2I & V2V.

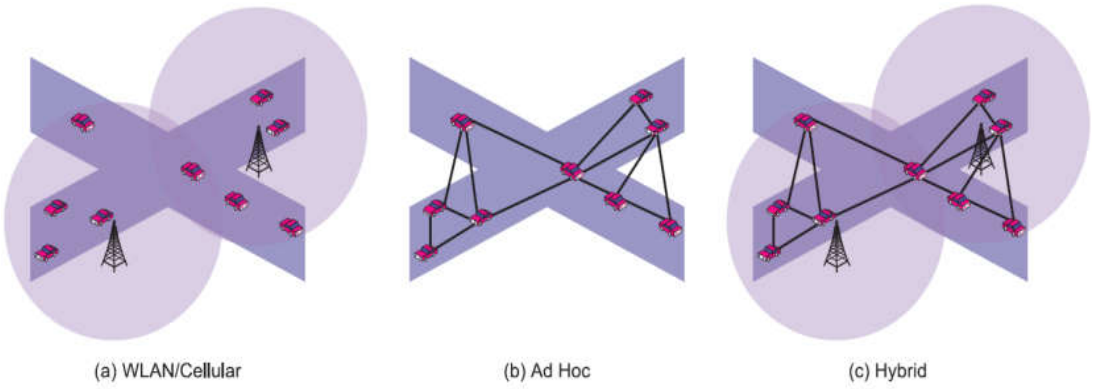


Figura 2.6 Arkitekturat e VANET

Një rrjet mobile ad hoc mund të jetë një rrjet mjaft i përshtatshëm për t'u aplikuar në PNs, jo vetëm për komunikime midis nyjeve personale në një P-PAN, por edhe për të ndërlidhur gjeografikisht nyjet e shpërndara që i përkasin grupimeve/klasterave të shumtë. Rrjetet mobile ad hoc mund të jenë arkitektura e rëndësishme e rrjetit në PNs për shkak të karakteristikave të tyre unike, të tilla si infrastrukturë-pavarësi, vetë-organizimi. Brenda një P-PAN ose klasteri/grupi, një rrjet mobile ad hoc është mjaft i përshtatshëm për shkëmbimin e të dhënave ndërmjet pajisjeve për shkak të thjeshtësisë dhe topologjisë dinamike të tij. Kur komunikimi ndër-grupor konsiderohet, çdo grup trajtohet si një rrjet celular i vogël, si në figurën më poshtë.

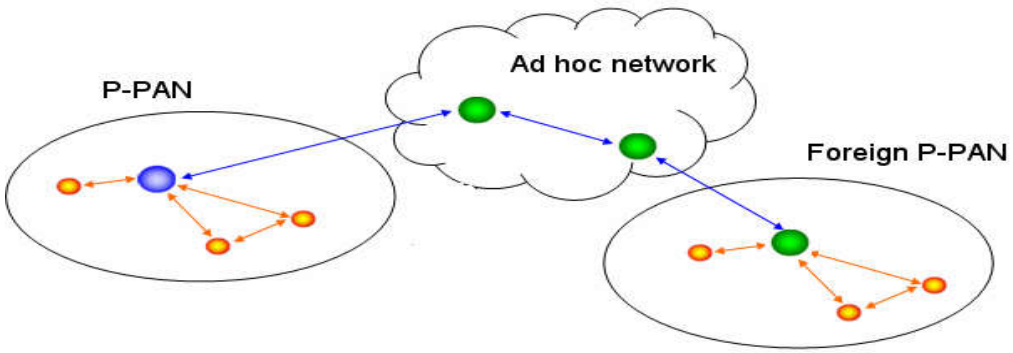


Figura 2.7. Komunikimi me nyjet e jashtme/huaja

Të gjitha këto rrjete mund të jetë të ndërlidhur përmes rrjeteve mobile ad hoc. Me fjalë të tjera, të gjitha nyjet e klasteruar mund të komunikojnë me njëri-tjetrin për të formuar një rrjeti mobile ad hoc. Kjo është e dobishme veçanërisht për komunikim me

PNs e personave të tjerë.(Qi Xu, May 2005). Edhe për këto lloje rrjetash ekzistojnë dy arkitektura të zakonshme, arkitektura hierarkike e rrjetit dhe arkitektura e sheshtë(Flat),të cilat i kemi trajtuar më lartë së bashku me karakteristikat dhe avantazhet e tyre.

2.3 Çështjet dhe Sfidat në Rrjetet Ad hoc Wireless

Çështjet kryesore dhe sfidat që ndikojnë në projektimin, zhvillimin, dhe performancën e rrjetit ad hoc wireless janë si më poshtë: **(**Yunus Khan and Dr. Sunita Varma, IEEE Transactions On Mobile Computing)

- *Skema e MAC(Medium Access Control)*
- *Rutimi*
- *Multicasting*[26]
- *Protokoll i Shtresës Transportuese*
- *Skema e Vënies së Çmimeve*
- *Cilësia e Shërbimeve, QOS(Quality of Service)*
- *Siguria e Vetë-organizimit*
- *Menaxhimi i Energjisë*
- *Adresim dhe Zbulim Shërbimi*
- *Shkallëzueshmëria*
- *Vlerësimi i Shpërndarjes /Marrja në konsideratë e Dislokimit*

Le t'i trajtojmë të gjitha këto çështje me rradhë:

- **Skema e MAC(Medium Access Control):** Në rrjet ad hoc, MAC shpërndahet dhe ndahet përmes kanalit për transmetimin e paketave. Për hartimin e një protokolli efikas MAC të merren parasysh çështjet e mëposhtme:
  1. Operacioni i shpërndarjes dhe sinkronizimi: Dizajni i protokollit MAC duhet të jetë plotësisht në një mënyrë të shpërndarë me kontroll minimal nga lartë duhet të jetë i sinkronizuar në kohë.

[26] Dërgimi i shumëfishtë i të Dhënave

2. Terminali i fshehtë: Terminalet e fshehta janë nyjet që janë të fshehura dhe jo të arritshme nga dërguesi i sesionit të transmetimit të të dhënave, por të arritshme nga terminali marrës. Prania e terminalit të fshehur zvogëlon prurjet e protokollit MAC në këtë mënyrë protokolli duhet të jetë në gjendje të trajtojë/përballojë efektet e terminaleve të fshehura.
3. Terminal i ekspozuar: Për të përmirësuar efikasitetin e protokollit MAC, nyjet e ekspozuara duhet të lejohen të transmetojnë pa shkaktuar përplasje në transferimin e të dhënave në vazhdim.
4. Prurjet: Protokolli MAC duhet ta ketë maksimizuar prurjen/xhiron e sistemit. Rritja e xhiros bëhet duke minimizuar shfaqjen e përplasjes, duke maksimizuar shfrytëzim e kanalit dhe duke minimizuar shpenzimet e përgjithshme të kontrollit.
5. Vonesa në akses: Vonesa në akses i referohet aftësisë së protokollit MAC për të ofruar bandwidth të barabartë për të gjitha nyjet konkurruese. Disa çështje të tjera të rëndësishme në MAC janë edhe çështje të tilla si drejtësia, mbështetje e trafikut në kohë, rezervimi i burimeve, aftësi për të matur disponueshmërinë e burimeve, aftësi për kontrollin e fuqisë, kontrollin e normës së përshtatjes, dhe përdorimin e antenave me drejtim.

Taksonomia e Protokolleve MAC:

- Protokollet e bazuar në lidhje
- Protokollet e bazuar në lidhje me mekanizëm rezervimi
- Protokollet e bazuar në lidhje me mekanizëm skedulimi
- Protokolle që përdorin antenat me drejtim
- MMAC (Multichannel MAC)
- MCSMA (Multichannel CSMA MAC Protocol0
- PCM (Power control MAC Protocol)
- RBAR (Recover based auto rate protocol)

➢ **Rutimi:** I referohet shkëmbimit të informacionit kurs dhe gjetjes së rrugës së duhur të mundshme në destinacion në bazë të kritereve të tilla si fuqi minimal e kërkuar, gjatësi hopit

dhe duke përdorur Bandwidth minimal. Sfidat kryesore të protokollit të rutimit janë si më poshtë:

1. Lëvizshmëria: për shkak të tiparit të lëvizshmërisë së nyjes thyerje të shpeshta të path_it, përplasje të paketave, lak(loop) i rastit që ndodhin në rrjet. Protokolli i rutimit duhet të jetë në gjendje të zgjidhë të gjitha këto probleme në mënyrë të efektshme.
2. Kufizim i Bandwidth: protokolli i rutimit duhet të jetë në gjendje që të ndajë dhe shpërndajë në mënyrë të barabartë bandwidth_in e rrjetit ndërmjet të gjitha nyjave në rajonin e transmetimit.
3. Pretendimi varet te vendndodhja (Location dependent contention): një protokoll i mirë rutimi duhet të ketë ndërtuar mekanizmin për shpërndarjen e ngarkesës në rrjet në mënyrë uniforme në të gjithë rrjetin e cila është e varur nga numri i nyjeve të rrjetit.

Kufizime të tjera burimesh: protokolli i rutimit duhet të jetë në gjendje që të trajtojë çështje që lidhen me llogaritjen e fuqisë, fuqinë e baterisë dhe magazinimin e buffer.

Kërkesat e protokollit të rutimit në rrjet ad hoc wireless:

Vonesë minimale e përvetësimit të kursit: Vonesa është e varur nga madhësia e rrjetit dhe nga ngarkesa e rrjetit.

Rikonfigurimi i shpejtë i path_it: nëse ndonjë ndryshim ndodh në rrjet për shkak të ndërprerjes së rrugës dhe humbjes së paketës, protokolli i rutimi të jetë në gjendje për rikonfigurim sa më shpejt të të jetë e mundur të rrjetit.

Rutim pa lak(loop free routing): Krijimi i lakut çon në humbje të bandwidth_it të rrjetit, kështu që protokolli i rutimit duhet të jetë në gjendje që të zbulojë lloje të tillë laqe_sh rastësor të rutimit dhe të marrë një veprim korrigjues.

Trajtimi i rutimit të shpërndarë: rrjeti ad hoc wireless përdor përqasjen e rutimit të shpërndarë për të dërguar paketat nga burimi në destinacion ndërmjet nyjeve celulare.

Kontrollin i sipërm minimal (Minimum control overhead): shkëmbimi i kontrollit të paketes është bërë me kontrollin e sipërm minimal të mundshëm.

Shkallëzueshmëria: shkallëzueshmëria është aftësia e një protokolli kurs për shkallëzim të mirë apo të performojë në mënyrë efikase në një rrjet me një numër të madh të nyjesh.

Sigurimi i QoS: një protokoll kursi duhet të jetë në gjendje të sigurojë një nivel të caktuar të cilësisë së shërbimit siç kërkohet nga nyjet, cilësia e parametrit të shërbimit mund të jetë bandwidth, vonesa, shqetësime, norma e dorëzimit të paketës dhe xhiroja.

Siguria dhe privatësia: protokolli i rutimit në rrjetet ad hoc wireless duhet të jetë në gjendje të trajtojë mohimin(kushtet) e shërbimit dhe sulmet në rrjet.

***Taksonomia e Protokolleve të rutimit për rrjetin Ad Hoc Wireless*:** protokolli i rutimit për rrjetin ad hoc wireless mund të klasifikohet në kategori të ndryshme në bazë të kritereve specifike. Protokollet kurs për rrjetin ad hoc wireless mund të klasifikohen në katër kategori në bazë të:

- Mekanizmit të përditësimit të informacionit të rutimit
- Përdorimit të informacionit të përkohshëm për rutimin
- Topologjisë së rutimit
- Përdorimit të burimeve specifike

Bazuar mbi mekanizmin e përditësimit të informacionit të rutimit: Protokollet proaktive ose të rutimit table driven. Protokolli i rutimit table driven ka aftësinë që çdo nyje të mirëmbajë informacionin e topologjisë së rrjetit në formën e tabelave të rutimit duke shkëmbyer periodikisht informacionin e rutimit. Informacioni i rutimit është i përmbytur në përgjithësi në të gjithë rrjetin. Kurdo që një nyje kërkon një path për një destinacion, ajo kryen një rrugë për gjetjen e algoritmit përkatës mbi informacionin e topologjisë që ajo mban.

- **<u>Multicasting[27] në rrjet ad hoc wireless:</u>**

Aplikacionet pa tel, si kërkimet emergjente, të shpëtimit dhe fushëbetejat ushtarake, ku shkëmbimi i informacionit është i detyrueshëm, kërkojnë protokolle rutimi të shpejta në dislokim dhe rikonfigurim, për shkak të këtyre arsyeve nevojiten protokollet e rutimit multicast. Në përgjithësi ekzistojnë dy tipe protokollesh rutimi multicast në rrjetat wireless.

[27] Dërgimi i të dhënave përmes një kompjuteri rrjeti në shumë përdorues njëkohësisht

Protokoll rutimi multicast bazuar në strukturë pemë, kjo lloj strukture mund të jetë shumë e paqëndrueshme në protokollet e rutimit ad-hoc multicast, pasi i nevojitet ri-konfigurim i shpesht në rrjetet dinamike, një shembull për këto lloje është shtesa multicast për AODV dhe ADMR. Lloji i dytë është protokolli multicast bazuar- mesh[28]. Protokollet e rutimit multicast bazuar-mesh janë më tepër se një path që mund të ekzistojë ndërmjet një çift burim marrës, CAMP (Core-asistuar Mesh Protocol) dhe ODMRP (On- Demand Multicast Routing Protocol) janë një shembull për këtë lloj klasifikimi. **(**Yunus Khan and Dr. Sunita Varma, IEEE Transactions On Mobile Computing)

Çështje të projektimit të protokollit multicast të rutimit:

Ka shumë sfida dhe karakteristika që duhen marrë në konsideratë kur zhvillohet një protokoll multicast rutimi, si: dinamika e topologjisë rrjetit, kufizimet e energjisë, kufizimi i shkallëzueshmërisë së rrjetit, dhe karakteristikat e ndryshme ndërmjet lidhjeve pa tel dhe lidhjeve me tel siç janë Bandwidth i kufizuar dhe siguria e dobët. Një protokoll multicast rutimi i mirë duhet të përfshijë karakteristikat si më poshtë:

- *Shkallëzueshmëria:* Protokolli multicast i rutimit duhet të jetë në gjendje të shkallëzohet për një rrjet me një numër të madh të nyjeve.
- *Sigurimi:* Autentifikimi i anëtarëve të sesionit dhe parandalimi i jo anëtarëve të fituar nga informacioni i paautorizuar luajnë një rol të madh në komunikimet ushtarake.
- *Fuqia:* Për shumë arsye, disa paketa të dhënash mund të rëzohen/bien në MANETs. Ky proçes rënie shkakton një raport/norm të ulët të dorëzimit të paketës. Për këtë arsye, një protokoll multicast rutimi duhet të jetë mjaftueshëm i fuqishëm për t'i bërë ballë lëvizjes së nyjeve dhe për të arritur një normë të lartë të dorëzimit të paketës.
- *Efikasiteti:* Efikasiteti Multicast përcaktohet si raport i numrit të përgjithshëm të paketave të marra nga marrësit me numrit e përgjithshëm të të dhënave të transmetuara dhe paketave të kontrollit në rrjet.
- *Kontrolli i sipërm:* Kufizimi i Bandwidth është shumë i rëndësishëm në MANETs. Kështu, hartimi i një protokolli multicast duhet të minimizojë numrin e përgjithshëm të paketave të kontrollit të transmetuara për mirëmbajtjen e grupit multicast.

[28] Bie në rjetë

- *Cilësia e shërbimit, QoS:* Është e domosdoshme në rutimet multicast në shumicën e rasteve dhe të dhënat e transferuara në një sesion multicast janë time-sensitive.
- *Varësia në protokollet e rutimit unicast*[29]*:* Ndonjëherë protokollet e rutimit multicast nevojitin të merren me rrjete të ndryshme, por është shumë e vështirë për protokollet multicast të punojnë në rrjetet heterogjene. Prandaj, protokollet e rutimit multicast janë të pavarur nga protokollet e rutimit unicast.
- *Menaxhimi i burimeve:* Në protokollin e rutimit multicast, menaxhimi i burimeve si menaxhimi i fuqisë dhe përdorimi i kujtesës janë çështje shumë të rëndësishme për ti mundësuar rrjetet ad-hoc të punojnë më mirë. Për të zvogëluar numrin e paketave të transmetimetuara, protokolli i rutimit multicast përpiqet të minimizojë burimin e fuqisë. Për të zvogëluar përdorimin e kujtesës, ai duhet të përdori informacionin minimal të gjendjes/shpallur

➢ **<u>Protokolli i Shtresës së Transportit</u>**

Objektivi kryesor i protokollit të shtresës së transportit është të krijojë dhe të mirëmbajë lidhjen fund -me- fund, shpërndarjen e besueshme fund - me - fund të paketave, kontrollin e rrjedhjes dhe kontrollin e kongjestionit. Ekzistojnë protokolle të shtresës së transportit të thjeshta, jo të besueshme, dhe pa lidhje siç është UDP, dhe protokolle të shtresës së transportit, të besueshme, bazuar nivel-byte, lidhje të orientuar të tilla si TCP për rrjetet me tel. Siç dhe mund të kuptohet protokollet e shtresës së transportit me tel nuk mund të jenë të përshtatshme për rjetat me ad hoc wireless. **(**Yunus Khan and Dr. Sunita Varma, IEEE Transactions On Mobile Computing)

Çështjet për Disenjimin e një protokolli të shtresës së transportit për rrjetet ad hoc Wireless:

- *Trafiku i detyruar:* Ndryshe nga rrjetet me tel, rrjetet ad hoc wireless shfrytëzojnë ritransmetimin radio multi-hop. Një transmetim në nivel link_u ndikon tek të dy nyjet fqinje të dërguesit dhe të marrësit të link_ut. Në një rrugë që ka lidhje të shumta, transmetimi në një lidhje të veçantë ndikon një link në rrjedhën e sipërme dhe një link në rrjedhën e poshtme. Pikërisht ky trafikut në ndonjë path të caktuar (ose rrugë), është

[29] Transmetimi i një pakete të dhënash ose i një sinjali audio vizual në një marrës të vetëm.

përmendur si trafiku i induktuar. Kjo është për shkak të natyrës së transmetimit të kanalit dhe diskutim lokacionit të varur në kanalin. Ky trafik ndikon tek xhirot e arritura nga protokolli i shtresës së transportit.

- *Ndërprerja e prurjes së parregullt/padrejtë:* Kjo i referohet parregullsisë së prurjes në shtresën e transportit për shkak vonesës të parregullt që ekziston në shtresat më të ulëta të tilla si shtresa e rrjetit dhe shtresa MAC. Për shembull, një rrjet ad hoc e wireless që përdor IEEE 802.11 DCF si protokoll MAC mund të përjetojë parregullsi të prurjes/ xhiros në shtresën e transportit. Një protokoll i shtresës së transportit duhet ti marrë parasysh këto në mënyrë që të sigurojë një ndarje të drejtë të xhiros përmes të gjithë flukseve konkurrente.
- *Ndarja e kontrollit të bllokimit të trafikut, besueshmëria dhe kontrolli i rrjedhjes*: Një protokoll i shtresës së transportit mund të sigurojë performancë më të mirë në qoftë se besueshmëria pikë me pikë , kontrolli i rrjedhjes, dhe kontrolli i bllokimit janë trajtuar veç e veç. Besueshmëria dhe kontrolli i rrjedhjes janë aktiviteteve pikë me pikë, ndërsa bllokimet mund me kohë të jenë një aktivitet lokal. Rrjedha e shtresës së transportit mund të përjetojë ngjeshje/bllokime me vetëm një link të ndërmjetëm nën ngjeshje. Për këtë arsye, në rrjete të tilla si rrjetet ad hoc wireless, performanca e shtresës së transportit mund të përmirësohet nëse këto trajtohen veç e veç. Ndërsa ndan këto, objektivi më i rëndësishëm për t'u konsideruar është minimizimi i kontrollit të sipërm shtesë të krijuar prej tyre.
- *Kufizimet e fuqisë dhe Bandwidth_it:* Nyjet në rrjetet ad hoc wireless përballen me kufizime të burimeve duke përfshirë dy burimet më të rëndësishme: burim e fuqisë dhe Bandwidth. Performanca e protokollit të shtresës së transportit është prekur ndjeshëm nga këto kufizime.
- *Keqinterpretimi i bllokimeve:*Mekanizmat tradicionale të zbulimit të ngjeshjes/bllokimit në rrjete, të tilla si humbja e paketës dhe ritransmetimi jashtë shërbimit, nuk janë të përshtatshme për zbulimin e bllokimet të trafikut në rrjetat ad hoc wireless. Kjo është për shkak se shkalla e lartë e gabimit të kanalit wireless, problemi i terminalit të fshehur, përplasjet e paketave në rrjet, rruga që prishet për shkak të lëvizshmërisë së

nyjeve, dhe dështimi i nyjeve për shkak të një baterie të drenazhuar mund të çojë në humbje të paketës në rrjetet ad hoc wireless. Për këtë arsye, interpretimi i rrjetit të ngjeshur siç përdoret në rrjetet tradicionale nuk është i përshtatshëm në rrjetet ad hoc wireless.

- *Shtresa e transportit e copëtuar plotësisht:* Një tjetër sfidë e hasur nga një protokoll i shtresës së transportit është ndërveprimi me shtresat më të ulëta. Protokollet e shtresës së transportit të rrjetit me tel janë pothuajse krejtësisht të tërhiqura nga shtresat më të ulëta. Në rrjetat ad hoc wireless, ndërveprimi ndër-shtresor midis shtresës së transportit dhe shtresave më të ulëta të tilla si shtresa e rrjetit dhe shtresa MAC është e rëndësishme për shtresën e transportit të përshtaten me mjedisin e rrjetit në ndryshim.
- *Topologjia dinamike:* Disa nga skenarët e dislokimit të rrjeteve ad hoc wireless përjetojnë ndryshime të shpejta të topologjisë së rrjetit për shkak të lëvizshmërisë së nyjeve. Kjo mund të çojë në ndërprerje të shpeshta të pathi_it, në ndarjen dhe rishfaqjen e rrjeteve, si dhe vonesa të larta në rithemelimin e rrugëve. Prandaj, performanca e një protokolli të shtresës së transportit është prekur ndjeshëm nga ndryshimet e shpejta në topologjinë e rrjetit.

➢ ***<u>Cilësia e Shërbimeve në rrjetet Ad Hoc:</u>***

Cilësia e shërbimit (QoS) është niveli i performancës i një shërbimi të ofruar nga rrjeti tek përdoruesi. Qëllimi i QoS është që të arrihet një sjellje më deterministe e rrjetit, në mënyrë që informacioni kryer nga rrjeti mund të dërgohet më mirë dhe burimet e rrjetit të mund të shfrytëzohen më mirë. Një rrjet ose ofrues i shërbimeve mund të ofrojnë lloje të ndryshme të shërbimeve për përdoruesit. Këtu, një shërbim mund të karakterizohet nga një grup i kërkesave të para-përcaktuara të matshme të shërbimeve të tilla si gjerësi minimale, vonesë maksimale, varianca e vonesës maksimale dhe norma maksimale e humbjes së paketës. Pas pranimit të një kërkese të shërbimit nga ana e përdoruesit, rrjeti duhet të sigurojë që kërkesat e shërbimit të rrjedhjes së përdoruesit janë përmbushur, sipas marrëveshjes, gjatë gjithë kohëzgjatjes së rrjedhjes (një lumë paketash nga burimi në destinacion). Me fjalë të

tjera, rrjeti duhet të sigurojë një sërë garancish të shërbimit ndërsa transporton një rrjedhje(një lumë paketash).

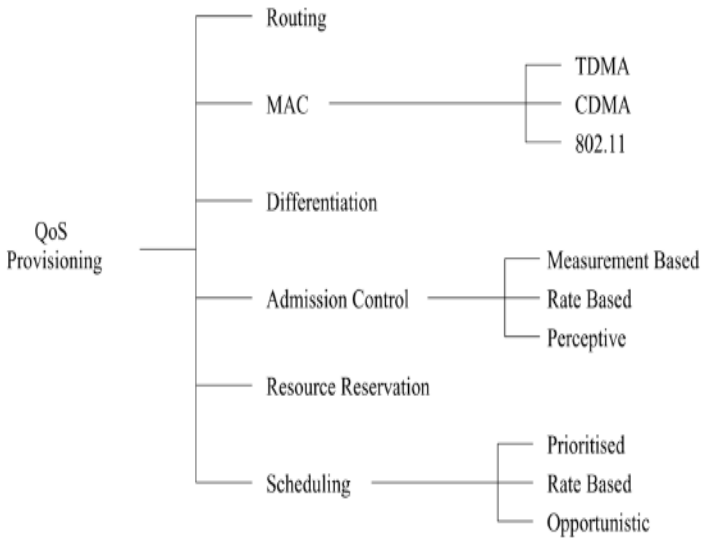


Figura 2.8. Cilësi e Shërbimit (QoS)

Pas pranimit të kërkesës të shërbimit nga ana e përdoruesit, detyra e parë është për të gjetur një rrugë të përshtatshme pa lak nga burimi në destinacion që do të ketë në dispozicion burimet e nevojshme për të përmbushur kërkesat QoS të shërbimit të dëshiruar. Ky proces është i njohur si rutimi QoS. Pas gjetjes së një rruge të përshtatshme, një protokoll rezervë burim është i punësuar që të rezervojë burimet e nevojshme në këtë kurs. Garancitë QoS mund të sigurohen vetëm me teknikat e duhura të rezervimit të burimeve.

Kualieti i Shërbimit (QoS):

- ✓ Bandwidth
- ✓ Vonesa
- ✓ Siguria
- ✓ Besueshmëria
- ✓ Prurja/Xhiroja
- ✓ Norma e shpërndarjes së paketës

Cilësia e Shërbimit informon rrugëzimin.

Cilësia e shërbimit bënë të vetëdijshëm protokollin e rutimit që të përdori parametrat e cilësisë të shërbimit (QoS)për gjetjen e një rruge/path_i. Vendimet e rutimit janë bërë në bazë të parametrave të cilësisë së shërbimeve të tilla si xhiroja e rrjetit, norma e ofrimit të paketës, besueshmëria, vonesa, norma e humbjes së paketës, norma e gabimeve bit dhe humbja e rrugës.

Kuadri i Cilësisë së Shërbimit:

Një kuadër për cilësinë e shërbimit është një sistem i plotë që përpiqet të ofrojë shërbimet e premtuara secilit përdorues apo aplikimit. Modeli i Cilësisë së shërbimit është komponent i rëndësishëm i kuadrit të cilësisë së shërbimit e cila përshkruan se si shërbimet janë shërbyer në përdorim. Çështja kryesore e dizenjimit është nëse i duhet shërbyer përdoruesit në një bazë për seancë ose një bazë për klasë. Çdo klasë paraqet një grumbull të përdoruesve në bazë të kritereve të caktuara. Komponenti tjetër i rëndësishëm i këtij kuadri janë të cilësia e shërbimit e rutimit për të gjetur të gjitha ose disa nga shtigjet e mundshme në rrjet që mund të plotësojnë kërkesat e përdoruesit, cilësia e shërbimit e sinjalizimit për rezervimin e resurseve të kërkuara nga përdoruesi ose zbatimin, cilësia e shërbimit të kontrollit të aksesit të mediumit, dhe caktimi i skemave që kanë të bëjnë me modelin e shërbimeve.

Taksonomia e përqasjeve të cilësisë së shërbimit:

Përqasjet e cilësisë së shërbimit mund të klasifikohen bazuar në ndërveprimin e shtresës së rrjetit dhe shtresës MAC, ose në bazuar në mekanizmin e përditësimit të informacionit të kursit. Bazuar në ndërveprimin midis protokollit të rutimit dhe mekanizmit të sigurimit të cilësisë së shërbimit, përqasjet e cilësisë së shërbimit mund të klasifikohen në dy kategori: përqasjet e shoqëruar dhe të ndara të cilësisë së shërbimit. Në rastin e parë, për kategorinë e parë, protokolli i rutimit dhe mekanizmi i sigurimit QoS ndërveprojnë ngushtë me njëri-tjetrin për kryerjen e garancive QoS. Nëse protokolli i rutimit ndryshon, mund të dështojë në sigurimin e mekanizmit të QOS.

Protokollet e rutimit të QOS(Quality of service) janë: TBP (Ticket based QoS routing), PLBQR (Predictive location based QoS routing protocol), TDR (Trigger based distributed QoS routing protocol), QoS AODV (Quality of Service enabled ad hoc on demand distance

vector routing protocol), BR (Bandwidth routing protocol), OQR (On demand QoS routing protocol), OLMQR (On demand link state multipath QoS routing protocol), AQR (Asynchronous QoS routing), CEDAR (Core extraction distributed ad hoc routing).

- **Vetë Organizimi:**

Vetë Organizimi është karakteristikë e rëndësishme e rrjetit ad hoc në të cilin kryhet organizimi dhe mirëbajtja e rrjetit në vetvete. Aktivitetet kryesore që i nevojiten një rrjeti ad hoc wireless për të kryer për vetë organizimin janë organizimi i topologjisë së zbulimit të fqinjit dhe riorganizimi topologjisë. Gjatë fazës së zbulimit të fqinjit çdo nyje në rrjet mbledh informacion në lidhje me fqinjët e saj dhe e mban këtë informacion në strukturat e duhura të të dhënave. Kjo mund të kërkojë transmetimin periodik të paketave të shkurtra të quajtur fenerë, të zhbiruesve të përzier në kanalin për zbulimin e aktiviteteve të fqinjëve. Disa protokolle MAC lejojnë ndryshme në fuqinë e transmetimit për të përmirësuar ripërdorimin e spektrit. Në fazat e organizimit të topologjisë çdo nyje në rrjet mbledh informacion në lidhje me të gjithë rrjetin ose një pjesë të rrjetit në mënyrë që të ruajë informacionin topologjik.

- **Menaxhimi i energjisë:**

Menaxhimi i energjisë është proçesi i menaxhimit të burimeve të energjisë për përmirësimin e gjithë jetës së rrjetit. Menaxhimi i energjisë ka të bëjë me kontrollin e burimeve të baterisë me anë të kontrollit të shkarkimit të baterisë, rregullimin e fuqisë së transmetimit, dhe caktimin e burimeve të energjisë. Menaxhimi i energjisë klasifikohet në kategoritë e mëposhtme:

Menaxhimi i fuqisë së transmetimit: Fuqia e konsumuar nga moduli i radio frekuencave të një nyje të lëvizshme përcaktohet nga disa faktorë si gjendja e operimit, fuqia e transmetimit, dhe teknologjia e përdorur për qarqet RF. Gjendja e operimit i referohet transmetimit, mënyrave të marrjes e të gjumit(sleep) të operacionit. Fuqia e transmetimit përcaktohet nga kërkesat e arritshme të rrjetit, të protokollit kurs dhe protokollit MAC të punësuar. Dizajni i hardware RF duhet të sigurojë konsumin minimal të energjisë në të gjitha tre gjendjet e funksionimit. Kalimi nga gjendja e fjetur kur transmetimi apo marrja

mund të bëhen nga hardware shtesë më pas një wake up(zgjim) bëhet për pranimin e sinjalit të kontrollit. . përgjegjësia e konservimit të energjisë qëndron në të gjithë shtresat e Link_ut të të dhënave, rrjetit, transportit, dhe të aplikimit. Duke projektuar një protokoll të shtresës së link _ut të të dhënave që redukton ritransmetimet e panevojshme, duke parandaluar goditjet, nga kalimi në modalitetin e pritjes apo modalitetin e fjetjes kur është e mundur, dhe duke pakësuar kalimin nga transmetim / marrje, kontrolli i enrgjisë mund të kryhet në shtresën e link_ut të të dhënave.

- *Menaxhimi i Energjisë së Baterisë:* Menaxhmenti i baterisë ka për qëllim zgjerimin e shtirjes së baterisë së një nyje duke përfituar nga vetitë e tij kimike, modelet e shkarkimit, dhe me zgjedhjen e një baterie nga një grup i baterive që është në dispozicion për tepricë teknologjike. Kontrolli i normës së ngarkimit dhe shkarkimit të baterisë është i rëndësishëm në shmangien e karikimit që në fillim me ngarkesë maksimale ose shkarkimin e plotë nën pragun minimal. Kjo mund të arrihet me anë të kontrollorëve të ngulitur në paketën e baterisë.
- *Menaxhimi i Fuqisë së Proçesorit:* Ora e fillimit dhe numri i udhëzimeve të ekzekutuara për njësi kohë janë disa nga parametrat e proçesorit që ndikojnë në konsumin e energjisë. Njësia qendrore e përpunimit mund të vihet në mënyra të ndryshme të kursimit të energjisë gjatë kushteve të ulët të përpunimit të ngarkesës. Fuqia e CPU mund të shndërrohet krejtësisht nëse makina është jashtë pune për një kohë të gjatë. Në raste të tilla, ndërprerjet mund të përdoren për të aktivizuar CPU pas zbulimit të ndërveprimit të përdoruesit apo ngjarjeve të tjera.
- *Menaxhimi i pajisjes së Fuqisë:* Menaxhimi i pajisjes Inteligjente mund të reduktojë konsumin e energjisë së një nyje celulare në mënyrë të konsiderueshme.

I. **Shkallzueshmëria:**

Në disa aplikacione (p.sh., fabrika me sensor mjedisor të mëdha, vendosjet e fushëbetejës, rrjetet e automjeteve urbane, etj) rrjeti ad hoc mund të rritet deri në disa mijëra nyje. Për rrjetet pa tel shkallëzueshmëria trajtohet thjesht me një ndërtim hierarkik. Lëvizshmëria e kufizuar e rrjeteve të infrastrukturës mund të trajtohet lehtë duke përdorur IP Mobile ose

teknikat vendore handoff[30]. Në të kundërt, për shkak të lëvizshmërisë më të gjerë dhe mungesës së referencave fikse, rrjetet e pastër ad hoc nuk tolerojnë IP mobile apo një strukturë të hierarkisë fikse. Kështu, lëvizshmëria, së bashku me shkallëzimin e madh është një nga sfidat më të rëndësishme në projektimin ad hoc.

Aplikimet tradicionale të tilla si ushtarake, operacionet e emergjencës dhe kontrollimit të turmës nuk mund të çojnë në një rrjet të tillë të madh ad hoc pa tel. Një sistem i bazuar në topologji hierarkike dhe adresimi mund të jenë më të përshtatshëm për rrjetet e mëdha ad hoc wireless. Rrjeti hibrid që kombinon ritransmetimi radio multi hop në praninë e infrastrukturës mund të përmirësojë shkallëzueshmërinë.

2.4 Siguria e Rrjetave Ad Hoc Wireless

Rrjetet ad hoc janë një paradigmë e re e komunikimit wireless për host_et mobile (të cilët ne i quajmë nyje). Në një rrjet ad hoc, nuk ka infrastrukturë fikse të tilla si stacionet bazë apo qendrat celulare komutuese. Nyjet Mobile që janë brenda rrezes radio të njëri-tjetrit komunikojnë drejtpërdrejt nëpërmjet lidhjeve pa tel, ndërsa ata që janë larg mbështeten në nyjet e tjera për të transmetuar mesazhe si router_a. Lëvizshmëria e nyjes në një rrjet ad hoc shkakton ndryshime të shpeshta të topologjisë së rrjetit. Për shkak të topologjisë dinamike në ndryshim mungesës së infrastrukturës, karakteristikave të decentralizuara, siguria është e vështirë të arrihet në rrjetet mobile ad-hoc. Për këtë arsye, mekanizmat e sigurisë duhet të jenë të ndërtuar në funksion të të gjitha llojeve të aplikimeve të rrjetit ad-hoc. Në këtë seksion, ne do të flasim për objektivat e sigurisë për aplikimet e dizenjimit, sulmet e mundshme kundër rrjetet ad-hoc dhe kundërmasat që tashmë janë propozuar.

Qëllimet e sigurisë: Për të siguruar një rrjet, zakonisht duhet të merren në konsideratë këto objektiva: disponueshmëria, konfidencialiteti, integriteti, autentifikimi dhe jo-mohim/refuzim.

[30] handoff- i referohet procesit të transferimit të një thirrje aktive ose sesion të dhënash prej një qelize nga një rrjet celular në tjetrin ose prej një kanali nga një qelizë në tjetrën. A handoff i zbatuar është i rëndësishëm për kryerjen e shërbimit të pandërprerë për një telefonues ose për seancën e të dhënave të përdoruesit.

Disponueshmëria:

Disponueshmëria është një kërkesë që siguron që sistemet të punojnë me përpikëri dhe shërbimi të mos i mohohet përdoruesit të autorizuar. Sulmet që ndikojnë në disponueshmërinë quhen mohimi i sulmeve të shërbimit (DoS). Në një rrjet ad-hoc, mohimi i sulmeve të shërbimit mund të nisë në çdo shtresë. Kundërshtari mund të përdori zhurmat për të ndërhyrë në komunikim në shtresën fizike. Në shtresën e rrjetit, kundërshtari do të mund të ndërpres protokoll e rutimit dhe shkaktojë shkëputje të rrjetit. Kundërshtari mund të shembë shërbime të nivelit të lartë. Duke çuar deri në shkarkimin e të gjithë baterisë.

Konfidencialiteti:

Konfidencialiteti është kërkesa që informacione private apo konfidenciale nuk duhet të zbulohen nga organe të paautorizuar. Transmetimi i informacioneve delikate, të tilla si informacione ushtarake strategjike ose taktike, por edhe informacione rreth transaksioneve financiare, kërkon konfidencialitet. Jo vetëm informacioni i nivelit të lartë duhet të mbetet konfidencial, por edhe informacioni i rutimit nuk duhet që të zbulohen, ky informacion mund të jetë i vlefshme për të identifikuar dhe gjetur objektiva në një fushë beteje, ose për të krijuar një profil të informacionit të një përdoruesi të veçantë.

Integriteti

Integriteti është vetia që të dhënat të mos ndryshohen në mënyrë të paautorizuar, ndërkohë që transferohen. Për të siguruar integritet, manipulimi i paautorizuar duhet të jetë i detektueshëm. Për shkak të ndërfaqes të komunikimit wireless një mesazh në një rrjet ad-hoc do të mund të korruptohet nga dështimet beninje/dashamirëse, si dëmtimi i përhapjes radio, ose për shkak të sulmeve dashakeqe në rrjet. Shpesh nuk është e lehtë të bëhet dallimi midis këtyre dy arsyeve për të dhënat e ndryshuara, për këtë arsye shumë kundërmasa që veprojnë për rrjetet me infrastrukturë fixe (p.sh. duke krijuar një nivel vlerësim për besueshmërinë e një nyje), nuk mund të zbatohen lehtësisht në rrjetet ad-hoc wireless.

Autentifikimi

Autentifikimi i mundëson një nyjeje të sigurojë identitetin e nyjes së afërt/kolege me të cilën është duke komunikuar. Kur transmetohen të dhëna konfidenciale, është e rëndësishme që nyja që merr informacionin është ajo që është menduar për të. Një nyjë mundet për shembull të shtiret/duket si një nyje tjetër dhe të fitojë akses të paautorizuar në burimet dhe informacione delikate. Në disa aplikime të rrjeteve ad-hoc, të tilla si pajisjet e komunikimit apo rrjetet sensor të lëvizshëm nq situata betejash, pajisja mund të manipulohet/ndryshohet, kështu që nuk mund të jetë vetëm e nevojshme për të vërtetuar pajisjen, por edhe duhet të sigurohemi se nuk ka qenë i kompromentuar.

Jo-mohimi

Jo-mohimi siguron se autor i një mesazhi nuk mund të mohojë që ka dërguar mesazhin. Ky qëllim është i një rëndësie të veçantë në të gjitha kërkesat e-commerce ose sa herë që pagesa dhe faturimi është i përfshirë. Përndryshe një përdorues do të mund për shembull të porositë një produkt ose shërbim, ndoshta pasi e përdorim e mohonë se ajo/ai ka urdhëruar ose pranuar atë produkt /shërbim kur ofruesi do ta faturojë këtë shërbim. Jo-mohimi është gjithashtu i dobishëm për zbulimin e nyjeve të kompromentuara. Kur një nyje A merr një mesazh të gabuar nga një nyje B, jo-mohimi i lejon A të akuzojnë B për përdorimin e këtij mesazhi dhe me këtë të bindë edhe nyjet e tjera që B është e kompрometuar.

2.4.1 Çështjet E Sigurisë Në VANETs

Siguria e rrjeteve ad hoc të automejteve (VANET) ka drejtuar më së shumti vëmendjen e përpjekjeve të kërkimit sot, ndërsa zgjidhje gjithëpërfshirëse për të mbrojtur rrjetin nga kundërshtarët dhe sulmet ende duhen përmirësuar, duke u përpjekur për të arritur një nivel të kënaqshëm, për shoferin dhe prodhuesin për të arritur sigurinë e jetës dhe vetkënaqësi. Nevoja për një rrjete të fuqishme VANET është fort i varur tek karakteristikat e sigurisë dhe privatësisë së tyre, të cilat do të diskutohen në vazhdim, më poshtë po japim tipet e sulmeve në VANETs:

1. *Mohimi i sulmit të shërbimt(DoS):* Ky sulm ndodh kur sulmuesi merr kontrollin e burimeve të një automjeti apo bllokimit e kanalit të komunikimit të përdorur nga rrjeti i automjetit, kështu që parandalon informacione kritike kur ato vijnë. Ai gjithashtu rrit

rrezikun për shoferin, në qoftë se ka varesi në informacionin e aplikimit. Për shembull, nëse një keqdashës do të krijojë një grumbull masiv deri në autostradë, ai mund të krijojë një aksident dhe të përdori sulmin DoS për të parandaluar paralajmërim që të brijë tek automjetet që afrohen.

2. *Sulmi i Shtypjes së Mesazhit* : Një sulmues në mënyrë selektive rrëzojnë paketat nga rrjeti, këto paketa mund të mbajë informacion të rëndësishëm për marrësin, sulmuesi i shtyp(duke i fshehur në një farë mënyre) këto pako dhe mund ti përdorin ato përsëri në një kohë tjetër. Qëllimi i një sulmues të tillë do të jetë parandalimi i autoritetet të regjistrimit dhe sigurimit nga të mësuarit në lidhje me përplasjet që përfshijnë automjetin e tij si dhe / ose për të shmangur dërgimin e raporteve të përplasjes në pikat e hyrjes në anë të rrugës. Pra kështu këta lloj sulmuesish nuk i lejojnë automjetet të marrin paralajmërim dhe ato janë të detyruar të presin në trafik.
3. *Sulmi ndaj Sajimit:* Një sulmues mund të bëjë këtë sulm duke transmetuar të dhëna të rreme në rrjetin, informacioni mund të jetë i rremë ose transmetuesi mund të pretendojnë se është dikush tjetër. Ky sulm përfshin sajime të mesazheve, paralajmërimeve, certifikatave, identiteteve.
4. *Sulmi i Ndryshimit:* Ky sulm ndodh kur sulmuesi ndryshon një të dhënë ekzistuese. Ky sulm përfshin vonesën e e transmetimit të informacionit, rishfaqjjen e transmetimit të hershëm, ose duke ndryshuar hyrjen aktuale të të dhënave të transmetuara. Për shembull, një sulmues mund të ndryshojë një mesazh duke u thënë automjete të tjera se rruga e tanishme është e qartë(e pa ngarkuar), ndërsa në të vërtetë rruga është e dyndur.

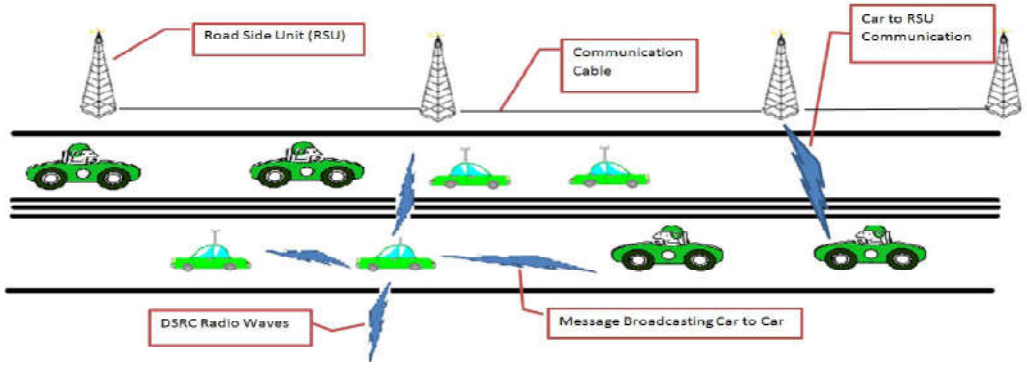


Figure 2.9. Struktura e VANET

5. *Sulm i Përsëritur:* Ky sulm ndodh kur një sulmues përsërit transmetimin e informacionit të mëparshëm për të përfituar nga situata e mesazhit në kohën e dërgimit. Siguritë bazë të 802.11 nuk kanë asnjë loj mbrojtje/efekti kundrejt përsëritjes. Ai nuk përmban numrat rendor apo vulat kohore(timestamps). Për faktin që çelësat mund të ripërdoren, është e mundur që të përsëriten mesazhe të ruajtura me të njëjtin çelës, pa zbulimin e futjes së mesazhit fals në sistem. Paketat individuale duhet të jenë të vërtetuara, jo vetëm të koduar. Paketat duhet të kenë vulat kohore(timestamps). Qëllimi i një sulmi të tillë do të jetë për të ngatërruar autoritetet dhe mundësisht pë të parandaluar identifikimin e automjeteve në goditje-dhe-ndodhje të incidenteve.
6. *Sulmi Sibil(Sybil):* Ky sulm ndodh kur një sulmues krijon një numër të madh të pseudonimesh dhe pretendimesh dhe vepron si të bëhej fjalë për më shumë se njëqind automjete, për ti treguar automjeteve të tjera se nuk ka bllokim përpara, dhe t'i detyrojë ato që të marrin një rrugë alternative. Një sulm Sibil varet në faktin se sa me lehtësi identitetet mund të gjenerohen, te shkalla në të cilën sistemi i pranon inpute nga subjektet që nuk kanë një zinxhir të besimit që i lidh ato me një entitet të besuar, dhe nëse sistemi i trajton të gjitha subjektet në mënyrë identike.

2.4.2 Çështjet E Sigurisë Në MANETs

Kërkesa të Sigurisë:Në vijim do të deklarojë dhe diskutojmë kërkesat kryesore të sigurisë së konfidencialitetit, integritetit dhe disponueshmërisë në kontekstin e MANETs.

Konfidencialiteti:

Konfidencialiteti garanton që përmbajtja e mesazhit të mos u shpallet kurrë subjekteve të MANET që nuk janë të autorizuar për ta interpretuar atë. Për shkak se linket wireless të MANETs janë lehtësisht të ndjeshëm ndaj përgjimit, konfidencialiteti është shumë i rëndësishëm për mbrojtjen e transmetimit të informacionit privat. Sidomos, ndonjë rrjedhje e të dhënave apo infomacion i trafikut të kontrollit (të tilla si rutimi) mund të jenë shumë të rrezikuara/dëmshme në rrethana të caktuara të tilla si raste emergjencash, ku jeta e njeriut është në rrezik. Në MANETs, konfidencialiteti bëhet më sfiduese, sepse nyjet e ndërmjetme mund të kenë nevojë për të përcjellë një mesazh nga një burim në një destinacion. Në këtë

rast, çdo nyje keqdashëse e MANET ka të ngjarë të provojë të zbulojë përmbajtjen konfidenciale të mesazhit si një hap i parë drejt llojet e ndryshme të sulmeve fizike ndaj rrjetit.

Integriteti:

Integriteti i mesazhit siguron që informacioni i transmetuar (të dhënat ose kontrolli) nuk është ndryshuar nga ndonjë entitet i paautorizuar. Ndonjëherë, ky ndryshim mund të ketë gabime për shkak të natyrës wireles të lidhjeve nga veprime me qëllim të keq kundrejt linkeve të MANET. Që të identifikohen dhe rimëkëmben nga gabime të tilla, protokolle të tilla si TCP dhe IP punësojnë checksums[31]. Megjithatë, një sulmues mund ti manipulojë të dhënat nga futje, fshirje ose zëvendësime. Autentifikimi i origjinës së mesazhit garanton identitetin e nyjeve të tjera të MANET që komunikojnë me të. Autentifikimi i njësisë është fokusuar në verifikimin e identitetit të nyjes pretenduese/paditëse të MANET nëpërmjet komunikimit aktual. Në një MANET, në qoftë se një atribut i tillë nuk është vendosur, një sulmues mund të maskohet si një nyje e ligjshme, prandaj është e mundshme që të ketë fituar akses të paautorizuar në burimet MANET. Nga ana tjetër, Autentifikimi i të dhënave ka të bëjë me verifikimin e origjinës së të dhënave. Prandaj, integriteti të dhënave është dhënë edhe nga ky aspekt.

Sulmet në MANETs

Ka kryesisht dy protokolle që përdoren në rrjetet Manet, protokoll i shtresës së Link_ut që përdoren për të siguruar lidhje ndërmjet nyjeve të ndryshme mobile për të siguruar lidhje një-hop_she, duke përdorur kanale wireless multihop. Nga ana tjetër, nëse duam të zgjerojmë lidhjet për HOPS të ndryshme të shumta atëherë rrjeti MANET përdor protokollin e shtresës së rrjetit.

Ka dy operacione kryesore të shtresës së rrjetit në MANET:

1. Rutimi Ad hoc

[31] Një checksum ose shuma hash është një nga të dhënat me madhësi të vogël nga një bllok i të dhënave dixhitale me qëllim zbulimin e gabimeve të cilat mund të jenë futur gjatë transmetimit të tij ose magazinimit. Ajo është aplikuar zakonisht në një skedar instalimi pasi është marrë nga download_imi serverit.

2. Transmetimi i të Dhënave të Paketës

Ata ndërveprojnë me njëri-tjerin dhe dërgimojnë paketën nga burimi në destinacion. Funksioni kryesor i protokolleve ad hoc të kurs është që të sigurojë rutimin ndërmjet nyjeve; ata shkëmbejnë mesazhe rutimi midis nyjeve të ndryshme të lëvizshme për të ruajtur informacionin e rutimit tek çdo nyje. Sipas gjendjes së rutimit, paketat e të dhënave të operimit të shtresës së dytë të rrjetit janë përdorur për të përcjellë të dhënat nga nyja e ndërmjetme e ardhshme e cila është një rrugë e vendosur për te nyja destinacion. Këto dy operacione janë të ekspozuara ndaj sulmeve keqëdshëse, dhe kjo do të çojë në lloje të ndryshme defektesh në shtresën e rrjetit.

Për shkak të kësaj arsyeje e rrjetit-shtresa në përgjithësi ndahen në dy kategori sulmet:

1. Sulmet e Rutimit
2. Sulme të shpërndarjes/transmetimit të paketës(bazuar në funksionimin e synuar të sulmeve)

Ka kategori të ndryshme të sulmeve të rutimit që nuk ndjekin specifikimin e protokollit të rutimit. Ekzistojnë protokolle të ndryshme të rutimit në MANET kështu pra dhe sjellje të ndryshme sulmi në lidhje me protokolle të ndryshme rutimi. Disa prej tyre janë diskutuar më poshtë:

1. Në bazë të kontekstit të protokollit të rutimit DSR kemi këto tipe te ndryshme sulmesh të paraqitura si më poshtë:
   - Një sulmues modifikon listën e rutimit burim në lidhje me paketat RREQ ose RREP.
   - Ndërrimi i rendit të nyjeve të ndryshme në listën e kursit.
   - Fshirja e hyrjeve nga lista.
   - Plotësimi i hyrjeve të nyjeve të rinj në listë.
2. Në bazë të kontekstit të protokollit të rutimit AODV, edhe këtu kemi disa sulme të ndryshme të cilat janë dhënë më poshtë:
   - Një sulmues reklamon rrugën me metrik të gabuar të distancës në lidhje me distancën aktuale për në destinacion.

- Reklamon përditësime të gabuara të rutimit kurs me një numër të madh rendor në lidhje me numrin aktual rendor.
- Një sulmues zhvlerëson të gjitha përditësimet kurs nga nyjet e tjera

3. Në bazë të kontekstit të protokollit të rutimit TORA, ka edhe metoda të ndryshme për sulmet:
   - Sulmuesit ndërtojnë path_e rutimi duke interferuar me mekanizma e protokolleve, psh kurset mund të detyrohen të përdorin sulmin ndaj nyjeve për të shkuar nëpërmjet tyre.
   - Sulmuesit mund të shterin burimet e rrjetit me veprimet keqdashse të injektimit, duke modifikuar dhe duke rëzuar paketat e të dhënave.

1. Sulmet Aktive

Ka edhe disa sulme aktive të ndryshme të cilat janë me të vërtetë të vështira për tu gjetur ose identifikuar për shkak se këto sulme janë më të sofistikuara dhe ato konsiderohen si sulme delikate të rutimit disa prej tyre janë dhënë më poshtë :

Sulmuesit mund të shkatërrojnë edhe më tej nyjet ekzistuese në rrjet.

- Ata mund të prodhojnë identitetin e tyre
- Ata mund të luaj rolin e nyjeve të tjera legjitime
- Sulmuesit në nyjet çift mund të krijojnë vrima depërtuese
- Ata gjithashtu krijon shortcut në flukset normale ndërmjet njëri-tjetrit
- Sulmuesit synojnë procesin e mirëmbajtjes së rrugës dhe reklamojnë që linku operative është thyer

Sipas kontekstit të sulmeve të rutimit ka edhe lloje të tjera sulmesh si sulmes që nisin sulme kundër operacioneve shpërndarëse të paketës, dhe për këtë shkak jo vetëm që do të ndërpresin protokollin e rutimit por gjithashtu infektojnë gjendjen e rutimit të çdo nyjeje. Për shembull, sulmuesi vendos rrugën dhe rrëzon paketën, ose gjithashtu modifikon përmbajtjen e paketave, apo dublikon paketat. Një tjetër lloj sulmi i shpërndarjes së paketës është sulmi i mohim-shërbimit (DoS) përmes prishjes së paketës së shtresës-rrjetit, në këtë lloj sulmi sulmuesi fut sasi të madhe të paketave të vjetëruara në sistem. Për shkak të këtij veprimi pjesë të konsiderueshme të burimeve të rrjetit humbasin, dhe normalisht

shkaktohen edhe bllokime në rrjet. Janë identifikuar dobësi të protokolleve të shtresës së Linkut, sidomos në protokollet 802.11 MAC të standartit IEEE, për rrjetin celular ad hoc. Është e vërtetë se 802.11 WEP është e ndjeshme ndaj llojeve të ndryshme të sulmeve kriptografike duke keqpërdorur primitivat kriptografike. Protokolli IEEE 802.11 është i ndjeshëm ndaj shumë sulme DoS synon skemat e rezervimit dhe zënien e kanalit. Sulmuesi shfrytëzon skemën backoff eksponenciale binare për të mohuar aksesin në kanalin wireless nga fqinjët e vet lokal.

2. Sulmet e Rutimit

Në përgjithësi ekzistojnë katër lloje të ndryshme të sulme të protokollit të rutimit MANET i cili është i ndarë në dy lloje kryesore të cilat janë dhënë më poshtë:

- Sulmet të ndërprerjes ë rutimit
- Sulme të konsumit të burimit

Në rastin e sulmeve të ndërprerjes së rutimit, detyra kryesore e sulmuesit është që të ndërpresi proçesin e rutimit me qëllim që të fusin path_et e gabuara. Në rast të sulmeve të konsumit të burimeve janë shqetësuese është detyra kryesore e sulmuesit për të futur disa nyje jo-bashkëpunuese apo 'egoiste' që mund të përdoren për të injektuar paketa të rreme në këtë mënyrë. Kryesisht të dyja këto sulme në protokollet e rutimit MANET janë shembujt më të mirë të sulmeve Denial of Service (DoS). Në figurën më poshtë është paraqitur një klasifikimi i gjerë i sulmeve në protokollet e rutimit MANET.

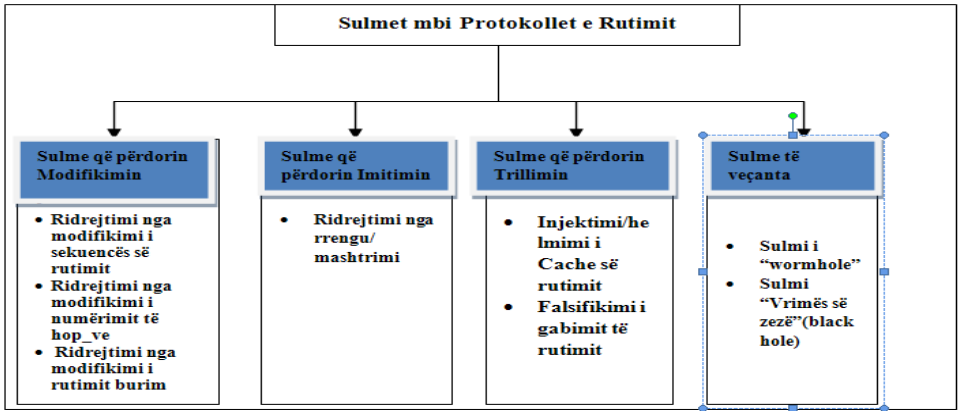


Diagrama 2.1 Klasifikimi i sulmeve në protokollet e rutimit MANET

3. Sulme që përdorin Modifikimin

Në rastin e sulmeve të tipit të modifikimit disa nga mesazhet në fushën e protokollit janë modifikuar dhe pastaj këto mesazhe kanë kaluar ndërmjet nyjeve, për shkak të kësaj mënyre shkaktohen përmbysje të trafikut, si edhe ridrejtimi i trafikut dhe gjithashtu vepron si një sulm i Mohimi të shërbimit (DoS). Disa nga këto lloje sulmesh janë dhënë më poshtë:

- *Modifikimi i numrave të sekuencës së rutimit*: Ky lloj sulmi është kryesisht i mundur kundrejt protokollit AODV. Në këtë rast një sulmues (p.sh nyje keqdashëse) përdoret për modifikimin e numrit rendor në paketat e kërkuara të rutimit.
- *Sumi i modifikimit të numërimit të hop_eve(hop count):* Në këto lloj sulmesh, ku dhe këto gjithashtu mund të jenë kryesisht kundrejt protokollit të rutimit AODV, këtu sulmuesi kryesisht ndryshon vlerën e numërimit të hop_ve duke u bërë shkak për tërheqjen e trafikut. Ata janë përdorur kryesisht për të përfshirë rrugë të reja, në mënyrë që të rivendosin vlerën e fushës numërimit të hop_ve në një vlerë më të ulët të një pakete RREQ ose ndonjëherë ajo është përdorur për tu vendosur në zero.
- Le të supozojmë se nyja S e cila vepron si një burim përpiqet të dërgojë një paketë të dhënash në drejtim të nyjes X, por nëse nyja M e ndërpret paketën dhe heq nyjen D nga lista dhe paketa shkon drejt nyjes C, ku nyja C do të përpiqet të dërgojë piketë në drejtim të X e cila nuk është e mundur, sepse nyja C nuk mund të komunikojë direkt me X, për këtë shkak nyja M ka krijuar me sukses një sulm DoS.
- *Sulmi i modifikimi të rutimit të Burimit:* Në këtë lloj sulmi që është i mundur kundër protokollit të rutimit DSR ku sulmuesi (nyja keqdashëse) modifikon adresën e burimit dhe e lëviz trafikun drejt destinacionit të saj. Në Figurën 2.10 përcaktohet mekanizmi, ku rruga më e shkurtër ndërmjet burimit S dhe destinacion X është përcaktuar (S-A-B-C-D-X). Ky path tregon se nyje S dhe nyja X nuk mund të komunikojnë me njëri-tjetrin direkt, dhe në skenarin (2.10) ku nyja M e cila vepron si një nyje keqdashëse do të bëjë të pamundurën për një sulm DoS.

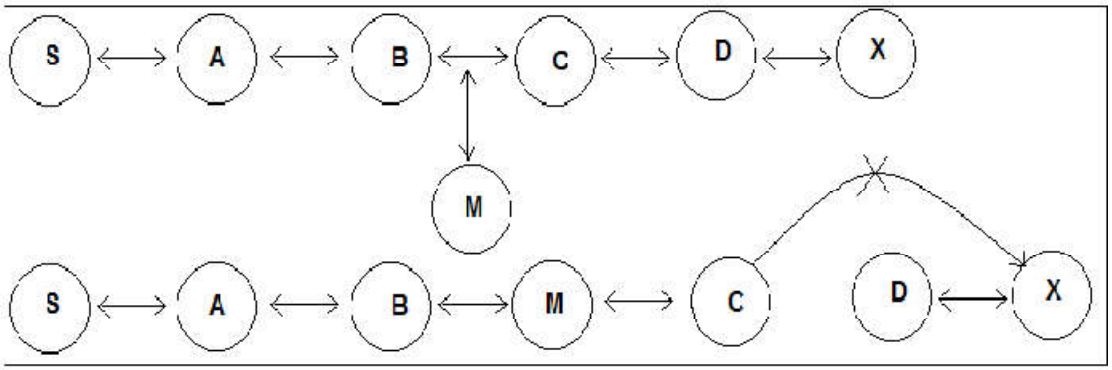


Figura 2.10. Një shembull i sulmit të modifikimit të rutimit

4. **Sulme që përdorin imitimin:**

Në këto lloje sulmesh sulmuesi është përdorur për të dhunuar autenticitetin dhe konfidencialitetin e një rrjeti. Në këtë sulm një sulmues (dmth nyje keqdashëse) përdor imitimin e adresës së nyjeve të tjera të përdoruesit për të ndryshuar topologjinë e rrjetit. Ky lloj sulmi mund të përshkruhet në figurën 2.11 të dhënë më poshtë:

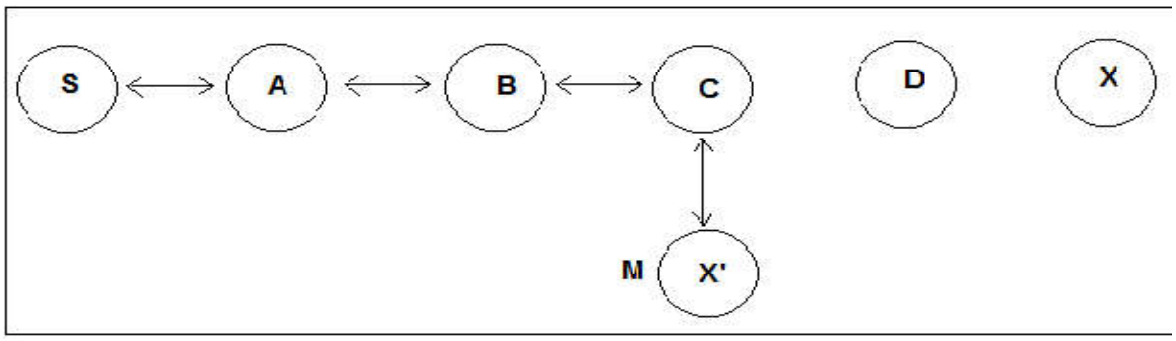


Figura 2.11. Një shembull i sulmit që përdorin imitimin

Në figurën e mësipërme ku nyja S dëshiron të dërgojë të dhënat drejt nyjes X dhe përpara se të dërgojë të dhënat në nyjen X fillon një proçes zbulim-rutimi. Gjatë procesit të zbulim-rutimit ka një nyje M keqdashëse, kur ajo të marrë paketën e zbulim rutimit lidhur me nyje X atëherë ajo modifikon adresën e saj dhe ndryshon, hiqet si nyja X, si nyje e shtirur e X si X'. Pas kësaj ai e dërgon paketën të pas në nyjen S burim duke i deklaruar se ajo është nyja destinacion nga kërkesa paketës RREP. Kur nyja burim merr informacionin e paketës

RREP kjo nuk do të autentifikoj/vërtetoj nyjen dhe e pranon rrugën duke dërguar kështu të dhënat në nyjen keqdashës. Ky lloj sulmeve quhet edhe sulmi lak(loop) i rutimit e cila do të bëhet shkaku i laqeve brenda rrjetit.

5. **Sulmet që përdorin rengun/trillimin***:*

Në këto lloj sulmesh, një sulmues si një nyje keqdashëse përpiqet të injektojë mesazhe të gabuara apo paketa rutimi të rreme në mënyrë që të prishi procesin e rutimit. Sulmet trillim janë shumë të vështirë për tu zbuluar në rrjetin mobile ad hoc. Në figurën 2.12, sulmet trillim shpjegohen me anë të një shembulli. Në shembull nyja burim S dëshiron të dërgojë të dhënat drejt nyjes destinacion X, kështu që për këtë arsye si fillim dërgon mesazhin e transmetuar dhe kërkesën për rrugën drejt nyjes destinacion X. Një sulmues si një nyje M keqdashës përpiqet të shtiret dhe të modifikojë rrugën dhe rikthen përgjigjen e rrugës në nyjen (S). Për më tepër, nyjet e një sulmuesi përdorin trillimin e kërkesave RERR dhe reklamojnë një shkëputje të nyjeve të linkut në një rrjet mobile ad hoc duke përdorur protokollet e rutimit AODV ose DSR.

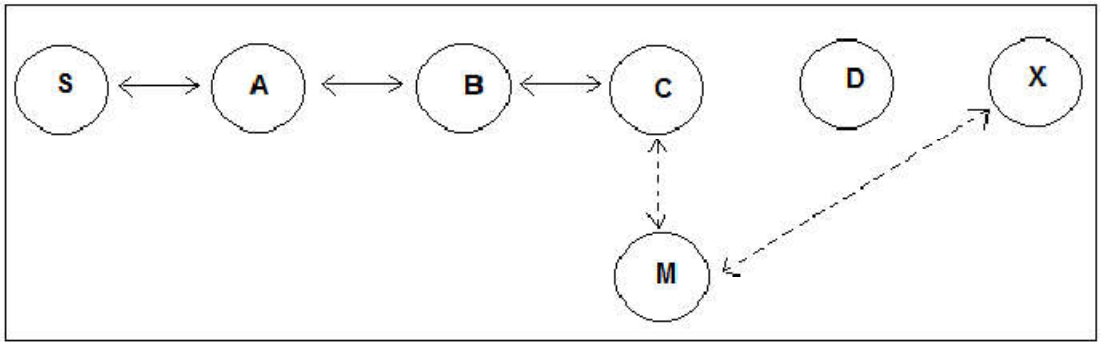


Figure 2.12. Shembull i sulmit të Fabrikimit

6. **Sulmet speciale**

Ka edhe disa sulme të tjera të ashpra në rrjetet MANET të cilat janë të mundshme kundrejt protokolleve të rutimit si AODV dhe DSR.

- *Sulmi Wormhole*[32]: Sulmi wormhole është një nga llojet e ashpra të sulmit në të cilin një sulmues fut dy nyje keqdashëse në rrjet, ku një sulmues përdoret për të përcjellë paketat nëpërmjet një "tuneli" private. Ky skenar i plotë përshkruhet në figurën 2.13, që është dhënë më poshtë:

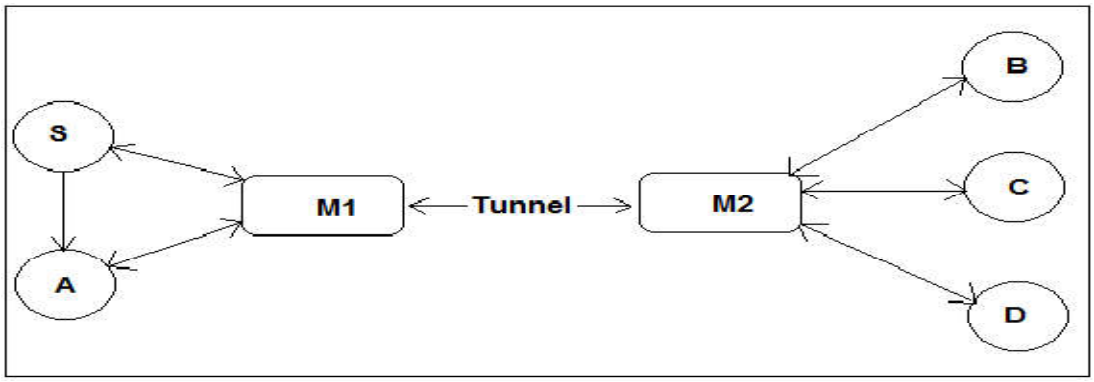


Figure 2.13. Shembull i sulmit Wormhole

- *Sulmi Vrimë Zezë(Blackhole):* Në këtë lloj sulmi, nyja përdoret për të reklamuar një zero metrike për të gjitha destinacionet, që bëhet shkak që të gjitha nyjet rreth saj t'i rrugëzojnë paketat e të dhënave në drejtim të saj. Protokolli AODV është i ndjeshëm ndaj këtij lloji sulmi, për shkak të vetive centrike që ka rrjeti, ku secila nyje e rrjetit duhet të ndajë tabelat e rutimit me njëra-tjetrën.

2.4.3 Kërcënimet kryesore të sigurisë që ekzistojnë në rrjetet ad hoc wireless:

Mohimi i Shërbimit: Për shkak të këtij sulmi burimi i rrjetit është i padisponueshëm për nyjet e tjera duke konsumuar Bandwidth ose mbingarkuar sistemin.

Konsumi i Burimeve: Konsumi i burimeve bëhet nga shterimi i energjisë së baterisë të nyjave duke përdorur trafikun e rënduar dhe mbiderdhjen e buffer. Në rast të sulmit të mbiderdhjes së buffer duke mbushur tabelën e rutimit hyrje/futje të padëshiruara ose të dhënat e paketave.

[32] Vrim që shkakton krimbi

Imitimi i Host_it: Një nyje e rreme vepron si një nyje e vërtetë dhe përgjigjet si një nyje e vërtetë apo origjinale dhe krijon hyrje të gabuara në tabelën e rutimit

Zbulim/demaskim i Informacionit: Një nyjë e kompromentuar mund të veprojë si një informatore me informacionin konfidencial të zbuluar për nyje të paautorizuar.

Interferenca: Një sulm i zakonshëm në aplikimin e mbrojtjes është ngjeshja e komunikimit wireless, duke krijuar zhurmë të gjerë të spektrit.

Siç u argumentua në siguri është një zinxhir, dhe ai është vetëm aq e sigurt sa dhe link_u më i dobët. Humbja qofë e një pike të vetme ndjeshëm çon në degradimin e forcës së sistemit të përgjithshëm të sigurisë.

Është gjithashtu e vërtetë se siguria nuk vjen falas. Për shkak të shumë karakteristikave të sigurisë, në rrjet, si rezultat do të rrisë llogaritjen, si dhe komunikimin dhe menaxhimin e lart gjithashtu. (Muhammad Ali Arshad & Yasir Sarwar, mars 2011)

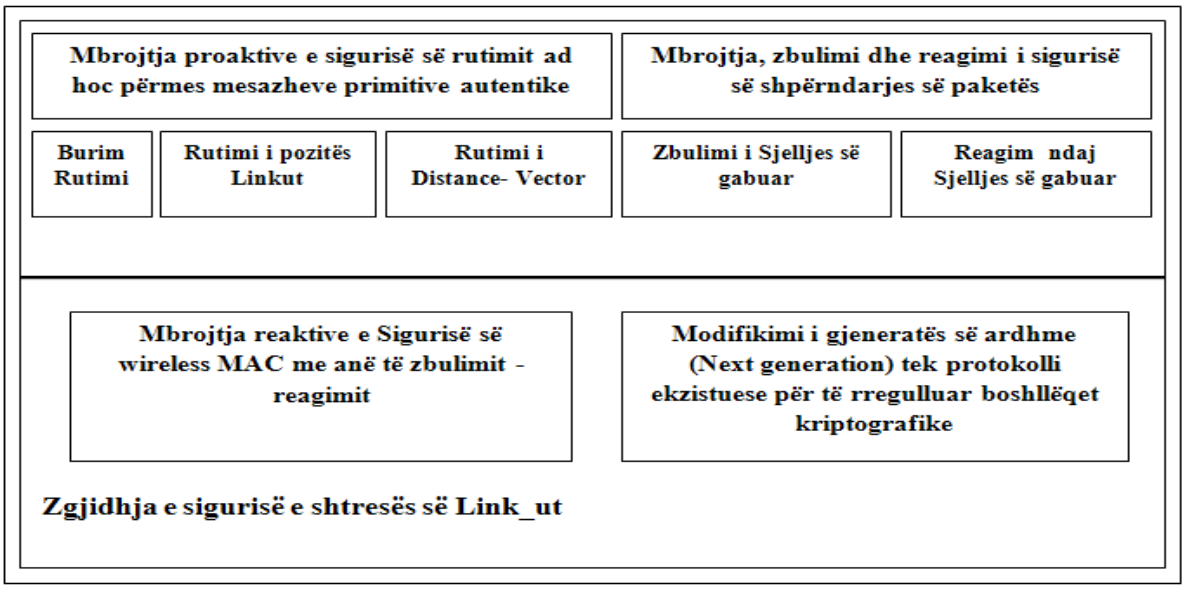


Diagrama 2.2. Komponentët në zgjidhje të Sigurisë

2.5 Sfidat

Veçoritë kryesore të rrjeteve ad hoc paraqesin disa sfida dhe mundësi në arritjen e këtyre qëllimeve të sigurisë:

- Së pari, përdorimi i lidhjeve wireless bën që një rrjet ad hoc të jetë i ndjeshëm ndaj sulmeve të linkut duke filluar nga përgjimet pasive në imitimet aktive, përsëritjen e mesazhit dhe shtrembërimin e mesazhit. Përgjimi mund ti japë një akses kundërshtarit ndaj informacionit sekret, duke shkelur konfidencialitetin. Sulmet aktive mund të lejojnë kundërshtarin që të fshijë mesazhet, për të injektuar mesazhe të gabuara, për të ndryshuar mesazhe, dhe të imitojë/luaj rolin e një nyje, duke shkelur kështu disponueshmërinë, integritetin, vertetësinë dhe jo-mohimin.
- Së dyti, nyjet, roaming në një mjedis armiqësor (për shembull, një fushëbetejë) me mbrojtje fizike relativisht të dobët të kenë probabilitet jo-të papërfillshëm në lidhje me të qënit i komprometuar. Prandaj, ne jo vetëm duhet të konsiderojmë sulmet me qëllime keqdashëse nga jashtë rrjetit, por gjithashtu të marrim parasysh edhe sulmet e lançuara brenda rrjetit nga nyjet e kompromentuara. Prandaj, për të arritur mbijetesë të lartë, rrjetet ad hoc duhet të kenë një arkitekturë të shpërndarë pa entitetet qendrore. Futja e çdo entiteti qendror në zgjidhjen tonë të sigurisë mund të shpinte në dobësi të rëndësishme; dmth në qoftë se ky entitet i centralizuar është i komprometuar, atëherë i tërë rrjeti çoroditet.
- Së treti, një rrjet ad hoc është dinamik për shkak të ndryshimeve të shpeshta në të dyja topologjinë dhe anëtarësimin e vet(dmth, nyjet shpesh bashkohen dhe lënë rrjetin). Marrëdhënia e mirëbesimit ndër nyjet gjithashtu ndryshonë, për shembull, kur nyje të caktuara janë zbuluar si të kompromentuara. Ndryshe nga rrjetet e tjera, nyjet në një rrjet ad hoc mund të bëhen lidhen dinamikisht me fushat administrative. Çdo zgjidhje e sigurisë me një konfigurim statik nuk do të mjaftojë. Është e dëshirueshme për mekanizmat tanë të sigurisë që të përshtaten shumë shpejtë me këto ndryshime. Së fundi, një rrjet ad hoc mund të përbëhet nga qindra madje edhe mijëra nyjet. Mekanizmat e sigurisë duhet të jenë të shkallëzuar për të trajtuar një rrjet të tillë të madh.

2.6 Konkluzione

Si një pjesë e përfundimit në bazë të vërejtjeve, rrjeti ad hoc wireless është zonë shumë e gjerë, në të cilën studiuesit mund të zbulojnë dhe të hetojnë gjërat e reja në çdo fushë. Në këtë studim gjejmë studime krahasuese të rrjetit celular dhe rrjetit ad hoc, zonat e aplikimit të rrjetit ad hoc wireless, rrjetit mesh wireless, rrjetit sensor wireless, rrjeti hibrid wireless, skemën e medium access të rrjetit ad hoc wireles, rutimin në rrjetin ad hoc wireless, multicasting në ad hoc rrjet pa tel, protokollet shtresa transport e ad hoc rrjet pa tel, skema çmimi i ad hoc rrjetit pa tel, cilësia e shërbimit të rrjetit ad hoc wireless, vetorganizimin, sigurinë, menaxhimin e energjisë në rrjetin ad hoc wireless, përparimet e fundit në rrjetet wireless.

Rrjetet Ad Hoc të Automjeteve(VANETs) janë një teknologji e re dhe premtuese, por kjo teknologji është edhe një rajon i favorshëm për sulmuesit, të cilët do të përpiqen për të sfiduar rrjetin me sulmet e tyre keqdashëse.

Kjo pjesë e dokumentit na dha një analizë të gjerë për sfidat aktuale dhe zgjidhjet, dhe kritikat për këto zgjidhje, gjithashtu u propozua një zgjidhje e re që do të ndihmojë për të mbajtur një rrjet të sigurt VANET, në punën e ardhshme ne duam të zgjerojmë idenë tonë për certifikatat e mesazheve të sigurisë, si duhen krijuar, fshirë, dhe verifikuar dhe duke i verifikuar dhe testuar ato me anë të simulimit. Rrjetet e automjeteve jo vetëm që do të ofrojnë siguri dhe aplikacione për të shpëtuar jetën, por ata do të bëhen një mjet i fuqishëm komunikimi për përdoruesit e tyre.

Në këtë punim të tezës jemi munduar që të merremi me çështjet e sigurisë në rrjetet ad hoc mobile(MANET). Një rrjet mobile ad hoc ka natyrën e hapur të mjeteve të komunikimit dhe lëvizjen e lirë që është arsyeja pse ajo ka nevojë të jetë më tepër e prirur për sa i përket rreziqeve të sigurisë p.sh ndërhyrjet, shpalosjet e informacionit dhe mohimi i shërbimit etj. Një rrjet mobile ad hoc ka nevojë për nivel të lartë të sigurisë, krahasuar me rrjetet tradicionale me tel. Përveç të tjerave në këtë temë u diskutuan karakteristikat e ndryshme të MANET dhe disa nga çështjet tipike dhe disa dobësi të rrezikshme në rrjetet mobile ad hoc. Qëllimi tjetër i kësaj çështjeje ishte diskutimi i aspekteve të ndryshme të sigurisë në MANET; së pari u diskutua mbi teknikat shumë-shtresore të zbulimit të ndërfutjes në rrjet

in multi hop te MANET; së dyti u diskutuan problemet e sigurisë që lidhen midis rrjetit multi hop dhe nyjeve celulare në rrjet mobile ad hoc. Pastaj kemi diskutuar disa nga llojet kryesore të sulmit të rrjetit të lëvizshëm ad hoc që është përdorur për të kërcënuar rrjetet. Ne gjithashtu arritën që të dimë se teknika e zbulimit të ndërhyrjes Multi-layer është e realizueshme në rrjetin multi-hop e MANET; përveç kësaj gjithashtu diskutuam probleme të ndryshme të sigurisë të cilat ndërlidhen ndërmjet rrjetit multi hop dhe nyjeve celular në rrjetin mobile ad hoc. Në fund, ne u morëm me protokollet e rutimit, sjelljen e ndërhyrësit dhe se si të merremi me ndërhyrësin dhe të implementojmë disa nga mekanizmat e sigurisë që mund të përdoren për të ndihmuar rrjetet mobile ad hoc nga kërcënimet e jashtme dhe të brendshme të sigurisë. Dhe si përfundim konkluduam se cili nga protokollet e rutimit është i përshtatshëm për mjedise të ndryshme, psh në qoftë se ne përdorim protokollin e përshtatshëm për një MANET, kështu i vështirësohet një infiltruesi sulmi ndaj rrjetit, p.sh në qoftë se ne kemi rrjet të madh alternativa më të mirë për këtë rast është përdorimi i protokollit AODV në krahasim me DSR dhe TORA, kjo ia bën shumë të vështirë një infiltruesi sulmin në rrjete të tillë, ndërsa në qoftë se ne kemi një rrjet të vogël por me lëvizshmëri të lartë mund të përdorim protokollin TORA, i cili performon më mirë duke rritur kështu masën e sigurisë në këto tipe rrjetesh. Me anë të kësaj pune ne zbulojmë se mund të sigurojmë një rrjet MANET në përdorimin e autentifikimit dhe pengesave të integritetit duke zbatuar Net doctor dhe mekanizmin e sigurisë së kërkesës në një server FTP për të bllokuar një përdorues jo të vërtetuar/autetntifikuar në MANET, por ka ende një problem që nëse një përdorues i autentifikuar vërtetuar fillon të ndryshojë sjellje/sillet keq është shumë e vështirë për ta gjetur këtë nyje apo nyje të tilla dhe për të bllokuar, por ne do të punojmë në të ardhmen në atë pjesë. Ne gjithashtu vërejtëm se në qoftë se ne kemi komunikimin ndërmjet dy MANETs, duhet përdorur firewall për të siguruar të dhënat ndërmjet dy MANETs, por për shkak të kohës së ulët të përgjigjes së faqes duhet gjithashtu të zbatohet lidhja VPN për të rritur kohën e përgjigjes së faqjes dhe enkapsuluar të dhënat, të cilat ofrojnë më shumë siguri.

Puna në të ardhmen

Megjithatë, në tezën tonë kemi pranuar se vlerësimi aktual për artin e zgjidhjeve së sigurisë wireless është thuajse ad hoc. Ka disa të meta të cilat duhet të përmirësohen dhe disa prej tyre janë dhënë më poshtë:

- Mungesa e mjeteve efektive analitike, veçanërisht në rast të vendosjes së rrjetit wireless në shkallë të madhe.
- Gjetja dhe bllokimi i një përdoruesi të autentifikuar, i cili fillon të humbasë sjelljet brenda rrjetit.
- Kompromiset shumëdimensionale midis forcës së sigurisë,
- Komunikimi i sipërm(overhead)
- Llogaritja e kompleksitetit
- Konsumi i energjisë,
- Shkallzueshmëria ende mbetet kryesisht e paeksploruar.

Duhet të zhvillohet një metodologji efektive vlerësimi dhe udhrrëfyese që ndoshta do të përdoret dhe do të ketë nevojë për përpjekje ndërdisiplinore nga komunitete të ndryshme kërkimore të cilat janë duke punuar në sistemet celular, cryptography, dhe rrjetet wireless. Në rastin e sigurisë kalimtare multicast është ende një problem i hapur.

KAPITULLI III: PROTOKOLLET E RUTIMIT AD –HOC

Për t'i kuptuar protokollet e komunikimit, bëjmë një krahasimin mes komunikimit të tyre dhe njerëzve. Që të mund të kuptohen dy njerëz duhet patjetër të flasin në të njëjtën gjuhë. Njëri person e fillon bisedën, psh. me një përshëndetje. Me këtë rast personat ndoshta do të duhen patjetër të merren vesh rreth "protokollit të komunikimit", d.m.th. gjuhës që do të përdorin. Personi tjetër (i dytë) pranon ftesën për bisedë dhe komunikimi është vendosur. Personat bisedojnë në atë menyrë që kur njëri flet tjetri dëgjon dhe nuk e ndërpret. Nëse të dy flasin njëkohësisht, komunikimi praktikisht është i pamundur. Në fund njëri nga personat dërgon një thirrje për përfundim të bisedës. Mbas pranimit të personit tjetër për përfundimin e bisedës, komunikimi ndërpritet. Kjo procedurë, e cila përmban rregulla të komunikimit të përcaktuara në mënyrë precize, njihet si " protokoll ". Në të njëjtën mënyrë, dy kompjutera mund të komunikojnë vetëm nëse "flasin" me të njëjtin protokoll.

Protokolli është një bashkësi rregullash të vendosura që bëjnë të mundur komunikimin e dy kompjuterave së bashku. Këto rregulla përfshijnë mënyrën se çfarë :

- metodë aksesi do të përdoret.
- topologjie fizike përdoret.
- lloje kabllosh mund të përdoren.

3.1 Protokollet E Rutimit Për Rrjetat E Lëvizshme Ad Hoc Wireless

Për të gjetur mënyrën më të mirë dhe për të rritur shkallën e komunikimit kjo varet nga aplikimet në jetën e vërtetë, prandaj në këtë punim shkencor kemi nevojë për të studiuar dhe krahasuar protokolle të ndryshme rutimi duke përdorur mbingakimin e rrjetit dhe konsumin e bandwidth si parametra të rëndësishëm dhe për këtë do të shfrytëzojmë rrjetat Ad Hoc Wireless.

Një numër i madh protokollesh janë zhvilluar për rrjetet ad hoc wireless që prej ardhjes të DARPA(Defense Advanced Research Projects Agency) rrjetave 'packet radio' në fillim të 1970_ës.(J. Jubin and J. Tornow vol. 75, no. 1, 1987, pp, 21-32).

Protokollet e rutimit në rrjetet packet-switched tradicionalisht përdorin ose algoritmin e rutimit distance-vector ose link-state. Dy prej tyre lejojnë një host[33] për të gjetur hopin tjetër apo të rradhës për të arritur në destinacion nëpërmjet asaj që është quajtur "rruga më e shkurtër". Si metrikë për "rrugën e shkurtër" mund të jetë numri i HOP_eve, vonesa kohore në milisekonda, numri i përgjithshëm i paketave në pritje përgjatë rrugës, etj... Këto protokolle me path më të shkurtër janë përdorur me sukses në shumë rrjete packet-switched dinamike. Në parim, çdo protokoll i tillë mund të përdoret gjithashtu edhe në rrjetet ad hoc.

E meta kryesore e të këtyre dy protokolleve distance-vector dhe link-state është se ata marrin shumë kohë për të konvergjuar dhe kanë një kompleksitet të lartë të mesazhit. Prandaj, për këtë shkak edhe të Bandwidth_it të kufizuar të lidhjeve pa tel, në një rrjet ad hoc kompleksiteti i mesazhi duhet mbajtur i ulët. Përveç kësaj, ndryshimi i shpejtë i topologjisë kërkon që protokollet kurs të mund të gjejnë rrugë të shpejta. Pra, protokollet e reja kurs duhet të zhvillohen për të përmbushur këtë filozofi themelore.

Në bazë të karakteristikave të tyre, këto protokolle në përgjithësi ndahen në dy tipe:

- **Table-driven**
- **Source-initiated(demand-driven)**

Në mënyrë skematike më poshtë paraqiten këto dy tipe protokollesh së bashku me "nën protokolle" të tjera që bëjnë pjesë në tipet që përmendëm më lartë:

[33]Host- Mikëpritës rrjeti që mund të ofrojë burimet e informacionit, shërbimet dhe aplikacionet për përdoruesit apo nyjet e tjera në rrjet.

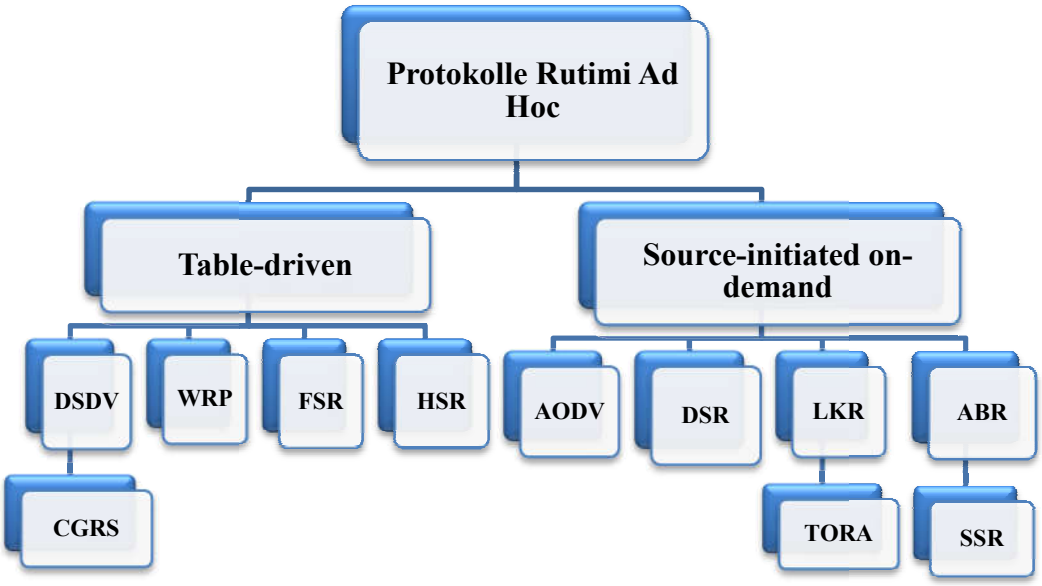


Diagrama 3.1. Paraqitja skematike e të dy tipeve të protokolleve të rutimit ad-hoc

Protokollet e rutimit Table - Driven përpiqen që të mbajnë qëndrueshmëri, dhe informacionin e rutimit(kursit) up-to-date në secilën prej nyjeve, pra nga njëra nyje në tjetrën në të gjithë rrjetin. Këto prokolle kërkojnë që për secilën nyje të mbajnë një ose më shumë tabela për të grumbulluar informacionin. Për të mbajtur një pamje të qëndrueshme të rrjetit, ndryshimeve në topologjinë e rrjetit këto protokolle iu përgjigjen duke propaganduar updates të rutimit në të gjithë rrjetin. Më poshtë do të trajtojmë disa prej këtyre protokolleve që bëjnë pjesë në protokollet Table – driven:

1. **(DSDV) Destination-Sequenced Distance-Vector Routing,** që është sqaruar në(J. Jubin and J. Tornow vol. 75, no. 1, 1987, pp, 21-32), është bazuar mbi mekanizmin e rutimit klasik Bellman-Ford. (L.R.Ford Jr. And D.R.Fulkerson, 1962). Është zhvilluar nga

Figura 3.1. Komunikim i thjesht ndermjet 3 nyjeve

C.Perkins dhe P.Bhagwat në 1994. Ideja ishte të zgjidhej problem I rutimit të ciklit(loop). Çdo hyrje në tabelën e rutimit përmban një numër rendor, numrat rendor janë nëse një link është present përndryshe një numër rastësor përdoret. Çdo nyje e lëvizshme në rrjet mban

një tabelë rutimi në të cilin të gjitha drejtimet e mundshme brenda rrjetit dhe numri i hop_eve janë të rregjistruara. Numrat e renditur i mundësojnë nyjeve të dallojnë ruterat e kaluara dhe të provuar më parë nga ato të reja, duke shmangur formimin e cikleve(loops) të rutimit. Ai adreson mangësitë lidhur me vetitë e varfra të ciklimit të mbyllur në RIP(protokoll i informimit të rrugëzimit) përballë lidhjeve të thyera. Modifikimi i përshtatur në DSDV e bën atë një protokoll kurs më të përshtatshëm për rrjetet ad hoc.
P.sh në këtë rrjet të thjeshtë, tabela e nyjes A do të ishte si më poshtë:[wiki]

Tabele 3.1. Paraqitja e hopeve të një nyje në një rrjet të thjeshtë.

Destinacioni	Hop_i tjetër	Numri i Hop_eve	Numrat rendor	Koha e vendosur
A	A	0	A 46	001000
B	B	1	B 36	001200
C	B	2	C 28	001500

Për të zbutur sadopak potencialin e sasisë së madhe të trafikut të rrjetit që updated mund të gjenerojnë, update_et router mund të përdorë dy lloje paketash.(E.Royer,Ch.K.Toh.,1999) E para është njohur si 'full dump', kjo lloj pakete mbart të gjithë informacionin e rutimit dhe kërkon njësi të dhënash për protokolle të rrjetit. Ndërsa lloji i dytë i paketave, paketa të vogla inkrementuese janë përdorur për të transmetuar vetëm atë informacion që ka ndryshuar që nga 'full dump' i fundit. Secili prej këtyre transmetimeve mund të përshtatet në masë standarte NPDU, duke zvogëluar sasinë e trafikut të gjeneruar. Broudcast_et[34] e ruterit të ri përmbajnë adresën e destinacionit, numrin e hop_eve që arrijnë destinacionin, numrin rendor të informacionit të marrë në lidhje me destinacionin. Përdoret gjithmonë ruteri i etiketuar me numrin rendor të fundëm.

Konsiderojmë një nyje burim S dhe një nyje destinacion D. Çdo hyrje e tabelë -rutimit në S është etiketuar me një numër rendor që e ka origjinën nga nyja destinacion. Për shembull, hyrja për D-në është etiketuar me një numër rendor që S e ka marrë nga D (ndoshta përmes

[34] Transmetime

nyjeve të tjera). Ne na nevojitet që të ruajmë qëndrueshmërinë e tabelave kurs në një topologji dinamike të ndryshueshme. Çdo nyjë periodikisht transmeton përditësime dhe kryhet nga çdo nyje kur informacion i ri i rëndësishëm është në dispozicion. Ne nuk supozojmë asnjë orë- sinkronizimi mes nyjeve celulare. Mesazhet e përditësimit tregojnë se cilat nyje janë të aksesueshme për secilën nyje dhe numrin e hops_ve për t'i arritur ato. Ne e konsiderojmë numërimin- hop si distancën midis dy nyjeve.

Megjithatë, protokolli DSDV mund të modifikohet për metrika të tjera. Ku një fqinj nga ana e vet kontrollon rrugën më të mirë nga tabela e vet e rutimit dhe ia përcjell mesazhin fqinjit të duhur të tij. Rutimi zhvillohet në këtë mënyrë. Ekzistojnë dy çështje në këtë protokoll:

a**.** Se si të ruajmë tabelat-kurs lokale.

b. Si të mbledhim informata të mjaftueshme për mirëmbajtjen e tabelave- kurs lokale.

a. Ruajtja e tabelave- kurs lokale

Ne së pari do të supozojmë se çdo nyjë ka të gjitha informatat e nevojshme për mbajtjen e tabelës-kurs të vet. Kjo do të thotë se çdo nyje e njeh të gjithë rrjetin si një grafik. Informacioni i nevojshëm është lista e nyjeve, kufijtë midis nyjave dhe kostoja e secilit kufijë. Kostot kufijë mund të përfshijnë: distancën (numri i hops_ve), normën e të dhënave, çmimin, bllokimet e trafikut ose vonesat. Ne do të supozojmë se kostoja kufi është 1 në qoftë se të dy nyjet janë brenda intervalit të transmetimit të njëri-tjetrit. Protokolli DSDV gjithashtu mund të modifikohet për kosto të tjera kufi.

b. Mirëmbajtja e tabelave të rutimit

Çdo nyjë mban tabelën e vet lokale të rutimit duke përdorur algoritmin e Bellman_Ford. Çdo nyjë 'i' mban, për çdo destinacion 'x', një grup të distancat 'dij (x)' për çdo fqinj 'j'. Nyja 'i' trajton të afërmit 'k' si hop të ardhshëm për një paketë të destinuara për 'x' në qoftë se 'dik (x)' është e barabartë me minimumin e të gjitha dij (x) kilxm (Jaya Bhatt, Naveen Hemrajani, nëntor 2013).

Mesazhi do të dërgohet nga *i* tek *l* si kosto minimale do të jetë path-i nga *x* përmes *l*.

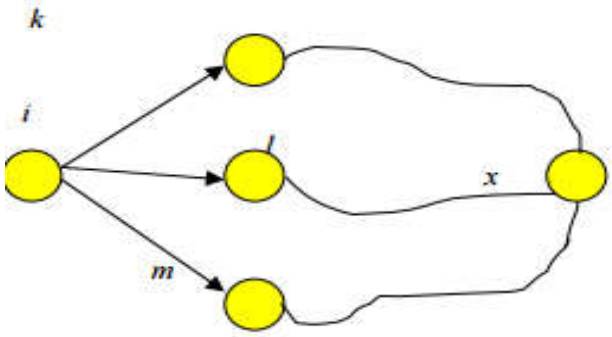


Figura 3.2. Lokalizimi i tabelës së rutimit për secilën nyjë.

DSDV (Problemi i Luhatjeve)

Cilat jane Luhatjet

4. Hyrja për D në A: [D, Q, 14, D-100]
5. Bën Transmetimi me seq. Nr. D-102
6. A merr nga P Update (D, 15 D-102)

-> Hyrja për D në A: [D, P, 15, D-102]

A duhet ta propagandojë/përhap këtë rrugë menjëherë**.**

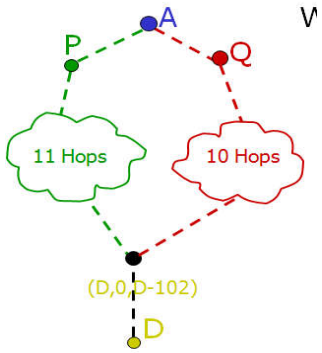


Figura 3.3 Luhatjet.

- A merr nga Q Update (D, 14, D-102),

  - Hyrja për D në A: [D, Q, 14, D-102]

A duhet ta përhap këtë rrugë menjëherë.

Kjo mund të ndodhë çdo herë që D apo ndonjë nyje tjetër bën transmetimin e saj dhe të çojë në njoftime rrugëtimi të panevojshme në rrjet, këto quhen luhatjet(fluktacione).

Si të shuhen luhatjet(fluktacionet)

- Regjistro kursin e fundit dhe të mesit. Bëhet vendosja kohë e çdo rrugëzimi në një tabelë të veçantë. (Të dhëna të qëndrueshme) Vendosje Kohe = Koha midis ardhjes së rrugës së parë dhe rrugës më të mirë me një numër sekuencial të caktuar.

- Lind pyetja a duhet ende të update_ojë tabelën e rutimit të vet mbi ardhjen e parë të një rruge me një numër sekuencial të ri, por ai mund të presi për ta reklamuar atë. Koha e pritjes është propozuar të jetë 2 * (Vendosje Kohe mesatare).

- Në rrjetet më të mëdha luhatje të tilla mund të shuhen për të shmangur shpalljet e panevojshme, duke kursyer bandwidth[35]

Kompleksiteti në DSDV:-Kompleksiteti kohë është O (d=diametër rrjetit), dhe kompleksitetin e komunikimit (Lidhje/dështimi linku) është O (N = numri i nyjeve të rrjetit)((Jaya Bhatt, Naveen Hemrajani, nëntor 2013). Performanca e DSDV kërkon që çdo nyje të mbajë dy tabela. Dhe pikërisht pjesa më e madhe e kompleksitetit në DSDV është për gjenerimin dhe ruajtjen e këtyre tabelave. Update/përditësimet u transmetohen fqinjëve periodikisht ose të planifikuar sipas nevojës. Me rritjen e lëvizshmërisë dhe numrit të nyjeve në rrjet, madhësia e bandwidth dhe tabelat e rutimit të nevojshme për të rinovuar këto tabela rriten njëkohësisht. Ngarkimet për mirëmbajtjen dhe përditësimin e këtyre tabelave do të rriten edhe ato njëkohësisht. Është e natyrshme që ngarkimet e larta të kursit do të pakësojnë punën e rrjetit.

Përmbledhje e protokollit DSDV:

- DSDV është proaktiv (Tabela Driven).
- Çdo nyjë mban informacionin kurs për të gjitha destinacionet e njohura.
- Informacioni Kurs duhet të përditësohet periodikisht.
- Trafiku i lartë edhe në qoftë se nuk ka ndryshim në topologjinë e rrjetit.
- Mban rrugët të cilat nuk janë përdorur.
- Mban thjeshtësinë e Distancë Vector.
- Garanton lirshmëri të ciklit(loop).
- Lejon reagim të shpejtë ndaj ndryshimeve topologjike.
- Çdo nyjë mban një tabelë-kurs i cili ruan metrikën e kostos së hop_it të ardhshëm drejt çdo destinacioni, si dhe një numër sekuencial që është krijuar nga vetë destinacioni.
- Çdo nyjë periodikisht përcjell tabelën e rrugëzimit për te fqinjët e saj.
- Çdo nyje rrit dhe bashkangjit numrin e vet rendor kur dërgon tabelë – kursin/rutimin e tij lokal.

[35] gjerësi e brezit

- Çdo rrugë është etiketuar me një numër rendor; rrugët me numër më të madh rendor janë të preferuara. Çdo nyjë reklamon një numër sekuencial çift me rritje monotonike për veten.

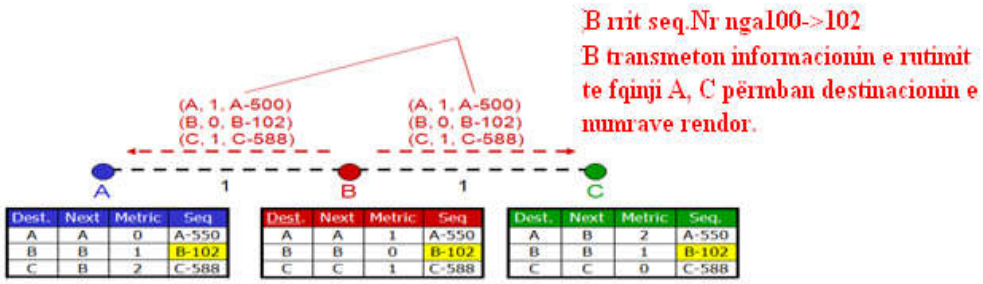


Figura 3.4. DSDV – Reklamim i rutimit

Rregullat për të vendosur informacionin e numrit rendor:

1. Në çdo reklamim/shpallje rritë vetë numrin rendor te destinacionit (përdorim vetëm numrat çift)
2. Nëse një nyje nuk është më e arritshme (timeout) rritë numrin rendor të kësaj nyje me 1 (numër rendor tek) dhe vendos metrikë = ∞

- Kur një nyje konstaton se një rrugëtim është thyer, ajo rrit numrin sekuencial/rendor të rrugëtimit dhe e reklamon atë me metrikë infinit.
- Destinacioni reklamon numrin e ri rendor.
- Stabiliteti dhe shkallëzueshmëria e DSDV garanton rutime me cikël – të lirë në paketat kurs. Ai përdor shuarje të plota dhe në rritje për përditësime. Përditësimi rritës është përdorur në mënyrë që të gjithë tabelat kurs të mos kenë nevojë që të transmetohen për çdo ndryshim në toplogjinë e rrjetit. Gjithësesi, DSDV kërkon periodikisht update të shuarjes se plotë, pavarësisht nga numri i ndryshimeve në topologjinë e rrjetit. Në këtë aspekt, DSDV nuk është efikas në update_et e rrugëtimit/kursit.
- Rutimi QoS me DSDV. Kërkesat e rutimi QoS në rrjetat ad hoc që mbështesin trafikun në kohë reale janë përmbledhur si më poshtë:

7. Rezervimi i brezit

8. Rutimi
9. Kontrolli i mbingarkesës:
10. Lëvizshmëria

2. CGSR(Clusterhead Gateway Switch Routing) – Protokolli CGSR ndryshon nga protokolli që përmendëm më lartë në mënyrën e adresimit dhe funksionimit të skemës së organizimit të rrjetit. Ky është një rrjet i lëvizshëm wireless me multihop_e të grumbulluar. (E.Royer,Ch.K.Toh.,1999) Përdoret një algoritëm për të zgjedhur një nyje që shërben si 'cluster head' duke përdorur një algoritëm shpërndarës brenda 'cluster'(tufës).

Në një sistem clustering[36], secili nga numërat e paracaktuara të nyjeve janë formuar në një cluster të kontrolluar nga një cluster head[37], e cila është caktuar duke përdorur një algoritëm të shpërndarë të clustering. Megjithatë, me skemën clustering, një cluster head mund të zëvendësohet shpesh nga një tjetër nyje, për disa arsye, të tilla si energjia e nivelit të poshtëm që mbetet në nyje ose një nyje lëviz jashtë kontaktit. Në këtë protokoll, çdo nyjë mban dy tabelat: një tabelë cluster- anëtarë dhe një tabelë kurs. Tabela cluster-anëtar regjistron kreun cluster për çdo nyje të destinacionit, dhe tabela kurs përmban hopin e ardhshme për të arritur në destinacion. Ashtu si me protokollin DSDV, çdo nyjë përditëson tabelën e cluster-anëtar me marrjen e një update të ri nga fqinjët e saj.

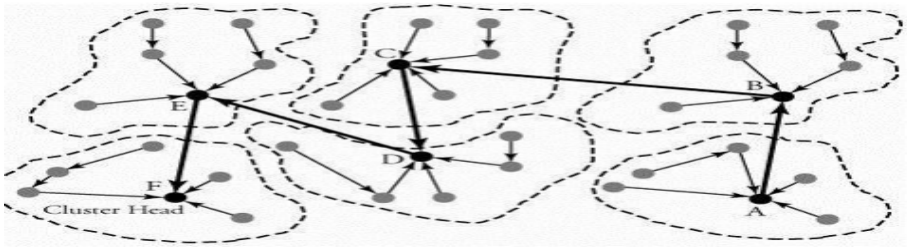


Figura 3.5. Komunikimi me protokollin CGSR (Communication with cluster-head gateway switch routing)

Disavantazhi qëndron në faktin se pikërisht në 'cluster head' frekuentë, ndryshimet mund të kenë efektin e kundërt në performancën e protokollit të rutimit ndërkohë që nyjet janë të

[36] grumbullimi
[37] Kreu-Klaster

zëna në përzgjedhjen 'cluster head' në vend që paketa të transmetohet. CGSR përdorin DSDV duke iu referuar si skemë themelore rutimit.

3. **WRP (The wireless Routing Protocol) –**qëllimi është të mbajë informacionin e ruterit në të gjitha nyjet e rrjetit(S. Murthy and J. J. Garcia-Luna-Aceves, Oct. 1996). Secila nyje është përgjegjëse në rrjet.Çdo nyje në rrjet është përgjegjëse për ruajtjen e katër tabelave:
   - Tabela për distancën (Distance table)
   - Tabela e rutimit(Routing table)
   - Tabela e Link – kosto(Link-cost)
   - Tabela e listës së mesazheve të ritransmetimit.(MRL)

Nyjet e lëvizshme informojnë njëra-tjetrën për ndryshimet në link duke përdorur update_in e mesazheve. Ky mesazh dërgohet ose shpërndahet ndërmjet nyjeve më të afërta dhe përmban një listë update_esh .Çdo path i ri kalon në nyjet origjinale të më parshme në mënyrë që dhe ato të update_ojnë tabelat në përpuhje me rrethanat. Në lëvishmëri kur merret një mesazh hello nga një nyje e re, kjo nyje shtohet në tabelën e rutimit të lëvizshëm dhe i dërgohet informacioni i tabelës së rutimit. Kjo ndihmon në eleminimin e situatës të cikleve(looping), duke përfituar një konvergjencë më të shpejtë kur ndodh një ngjarje dështim-linku.

4. **HSR(Hierarchical Routing Protocols)**

Lidhja i referohet mbajtjes së të gjithë rrjetit, lëshimin e përditësimeve të rutimit, duke mbajtur gjurmët e nyjeve që hyjnë dhe dalin në rrjet etj. Me rritjen e madhësisë së MANET, rritet gjithashtu edhe trafiku i kontrollit. Kur nyjet janë të ngarkuar me gjetjen e rrjetit si dhe të transferimit të të dhënave, bottlenecks[38] janë krijuar brenda rrjetit kryesor jo vetëm në daljen nga puna të baterisë, por dhe në performancën e ngadaltë të rrjetit.

Prandaj është shumë e rëndësishme që të distancojmë të dyja këto funksione për të parandaluar dështime të nyjes për shkak të vështirësive dhe të kushteve të ulta të energjisë siç shihet në modelet hierarkike. Ne gjithashtu kemi për të zgjidhur problemin e

[38] Pengesa

scalability[39]. Kjo mund të bëhet duke ndarë Manet në grupe me një që ngarkohet me përgjegjësi të detyrueshme. Grupimi brenda MANETs është thelbësore pasi ai i dekurajon tabelat e mëdha kurs. Secili sektor mund të ketë vetëm një numër të kufizuar të nyjeve celular që cluster-head mund të mbështesi. Nëse numri tejkalohet një tjetër cluster mund të jetë krijuar me një cluster-head. Kjo gjithashtu kufizon trafikun e kontrollit brenda sektorit. Claster-head i secilit sektor është i lidhur me claster-head të grupimeve fqinje të tij të menjëhershme nëpërmjet një nyje portë (shih figurën 3.6). Cluster-heads nuk marrin pjesë në transferimin e të dhënave, përgjegjësia kryesore e tyre është të lidhin cluster dhe të mbajnë updated tabelat e rutimit. Kjo gjithashtu e ruan clusterhead nga ikja/mbarimi i energjisë dhe shmang krijimin e bottlenecks në pathin e rutimit që ndodhë për shkak të trajtimit të dy detyrave.

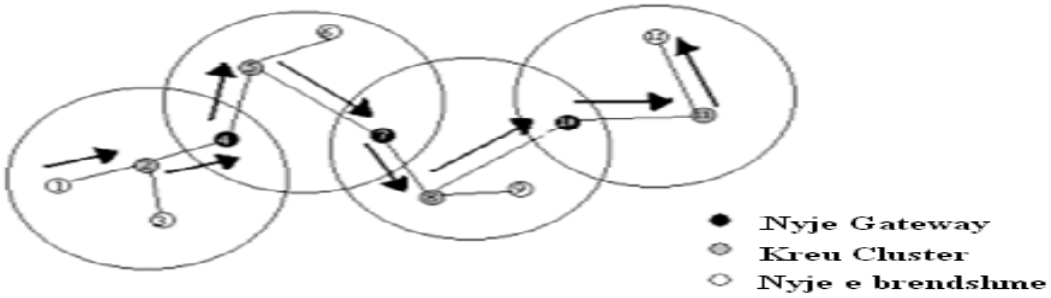


Figura 3.6. Ndarja hierarkike e rrjetit

Rrugëzimi në kurset e protokollit HSR mund të jetë dy llojësh; e parë që përfshin vetëm një cluster, dhe i dyti, që përfshin cluster të shumëfishta. Në rastin e rrugëzimeve që përfshin cluster të shumëfishta, e gjithë rruga është e ndarë në segmente. Ky rrugëzim aktiv menaxhohet në mënyrë hierarkike duke përdorur dy protokollet

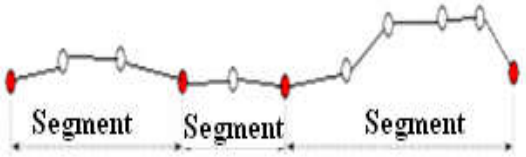


Figura 3.7. Segmentimi i Rrugës

[39] Shkallëzueshmërisë

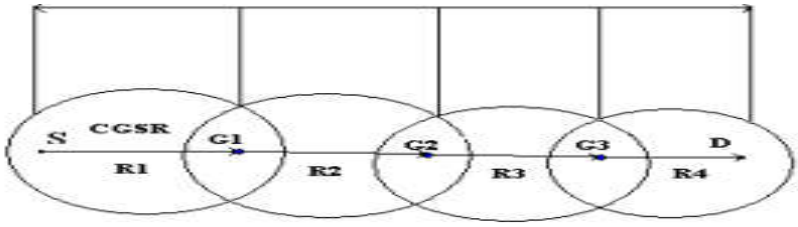


Figura 3.8. Rrugëzimi nga Burimi “S” në Destinacionin “D”

kurs; një në nivel inter-segmentit dhe tjetri në nivel intrasegment. E gjithë rruga nga burimi në destinacion ka nyjet që përfshijnë cluster të shumëfishta dhe janë të ndara në segmente. Një segment është një pjesë e një rruge që formon një pjesë të një claster_i të caktuar. Kjo është rruga midis dy nyjeve portë apo rruga midis nyjes portë dhe nyjes burim apo nyjes destinacion. Me fjalë të tjera, një rrugë është një lidhje e një ose më shumë segmenteve dhe segmenti ka një kokë- segment. Ku informacioni i nevojshëm për të ruajtur kursin është dhënë në nyjen qendrore segment nga kreu- cluster i kësaj zone. E gjithë rruga reduktohet në një lidhje një dimensionale të segmenteve që përfshin shumë cluster-a nga burimi në destinacion. Siç tregohet në figurën 3.6 nyjet kre-cluster nuk formojnë një pjesë të itinerarit të kursit. Nyjet e errëta që janë treguar në figurën 3.6 janë nyje cluster- portë që ndërfaqosin dy cluster- fqinje. Gjithashtu vini re se nuk ka nyje cluster header pjesëmarrëse në këtë kurs. Ndërsa DSR përcakton itinerarin e plotë nga burimi në destinacion. Në HSR vetëm adresat e nyjeve portë specifikohen siç tregohet në figurën 3.8 e cila tregon një krahasim të rrugëzimit të kreut ndërmjet HSR dhe CGSR gjatë 'udhëtimit' të paketës nga Burimi "S" në Destinacion “D”. Vini re se CSR është zbatuar në nivel intra-cluster dhe DSR në nivel inter-cluster. Hierarkike, rrugët menaxhimit mund të jetë e dobishme kur është fjala deri te paketa e sipërme dhe duke minimizuar vonesën pikë me pikë(end-to-end). Në protokollet e sheshtë kurs, sa herë që një nyje pjesëmarrëse bie jashtë apo bëhet joaktive gjithë rruga duhet të themelohet. Me rritjen e madhësisë së MANET rrugët bëhen më të gjatë dhe thyehen më shpesh. Kjo shkakton harxhim të madh të burimeve dhe kohës. Ku si në rastin e zgjidhjes së propozuar, sa herë që një dështim nyje ndodh për ndonjë arsye ajo mund të riparohet në vend, pa pasur nevojë të hidhet poshtë itinerari i plotë i rrugës. Kjo kursen shumë kohë dhe në masë të madhe zvogëlon rrjetin e lartë të panevojshëm. Prandaj dy

protokollet janë shkrirë së bashku në këtë hierarki duke zbatuar CGRP në nivel intra-segment dhe DSR në nivel inter-segment. Më poshtë po paraqesim dy kurset:

Kursi DSR	**Kursi HSR**
1.At Source S–D R4 G3 R3 G2 R2 G1 R1	1. At Source S – D G3 G2 G1 R1
2. At G1 – D R4 G3 R3 G2 R2	2. At G1 – D G3 G2 R2
3. At G2 – D R4 G3 R3	3. At G2 – D G3 R3
4. At G3 – D R4	4. At G3 – D R4

5. Protokolli FSR

FSR(Fisheye Shteti Routing) është një protokoll implicit hierarkik kurs. Gjithashtu konsiderohet si një protokoll proaktive dhe është një protokoll kurs i bazuar në gjendjen e linkut(link-state) që është përshtatur me mjedisin ad hoc wireless. Nyjet shkëmbejnë hyrjet e link state me fqinjët e tyre me një frekuencë e cila varet nga distanca për destinacion.

Ky protokoll përdor teknikën "fisheye"(teknika e Peshkut) e propozuar nga Kleinrock dhe Stevens (L.Kleinrock and K.Stevens,1971), ku kjo teknikë është përdorur për të zvogëluar madhësinë e informacionit që kërkohet për të përfaqësuar të dhënat grafike. Syri i një peshku kap me hollësi të lartë pixel_at pranë pikë fokale/qëndrore. Detaji zvogëlohet ndërsa distanca nga Pika Fokale rritet. Në kurs, përqasja fisheye përkthehet në ruajtjen e saktë të distancës dhe informacionit e cilësisë së rrugës në marrëdhënie fqinjësie të drejtpërdrejta të një nyje, me më pak detaje në mënyrë progresive me rritjen e distancës.

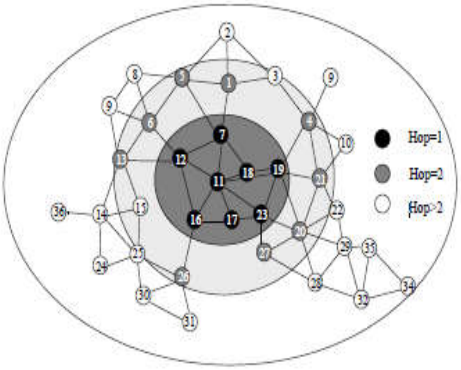


Figura 3.9 Paraqitje e teknikës "Fisheye"

FSR është funksionalisht i ngjashëm me rugëtimin LS (Link State) në atë që ajo mban një hartë topologjie në çdo nyje. Në LS, paketat janë gjeneruar dhe përmbytur/vërshuara në rrjet sa herë që një nyje zbulon një ndryshim topologji. Në FSR, paketat link- state nuk janë

të vërshuara. Në vend të kësaj, nyjet mbajnë një tabelë link-state bazuar në informacionin up-to-date të marra nga nyjet fqinje, dhe periodikisht e shkëmbejnë atë vetëm me fqinjët e tyre lokale (pra nuk ka vërshime). Tabela periodike e shkëmbimit FSR i ngjan vektorit shkëmbimit në Distributed Bellman-Ford (DBF), në një ambient pa tel, një lidhje radio midis nyjeve celular mund të përjetojnë shkëputje të shpeshta dhe rilidhje. Protokolli LS lëshon një përditësim të link-state për çdo ndryshim të tillë, i cili përmbyt rrjetin dhe shkakton prurje të larta. FSR shmang këtë problem duke përdorur këmbimin periodik të hartës topologjike, duke reduktuar në masë të madhe ngarkesen e mesazh kontrollit. Kur madhësia e rrjetit rritet shumë, mesazhi përditësimit mund të konsumojë sasi të konsiderueshme të Bandwidth, e cila varet nga periudha e përditësimit. Në mënyrë që të zvogëlojë madhësinë e mesazheve të përditësimit pa ndikuar seriozisht saktësinë e kursit, FSR përdor teknikën Fisheye (shih Fig. 3.9) të shpjeguar më lartë.

Siç e theksuam diçka edhe më lartë protokollet që bëjnë pjesë në këtë grup mbështeten në një mekanizëm update$_{imi}$ të tabelës së rutimit që përfshin përhapjen konstante të informacionit të rutimit. Kur një nyje i nevojitet një kurs për një destinacion të ri asaj i duhet të pres derisa ky ruter apo kurs të zbulohet. Nga ana tjetër duke qenë se i gjithë informacioni përhapet në mënyrë konstante dhe mbahet në protokollet e rutimit table-driven, një kurs për secilën nyje në rrjetat ad hoc wireless mbahet në dispozicion, pavarësisht nëse është apo jo e nevojshme. Të gjitha protokollet që permendëm përveç CGSR përdorin skemë adresimi monoton ose të sheshtë (flat), faktikisht ky lloj adresimi është më pak i komplikuar dhe më i lehtë për tu përdorur.

Protokollet e rutimit Source–Initiated On–Demand - Ky lloj rutimi krijon ruterat(rrugët) vetëm kur këtë e kërkon nyja burim. Kur një nyje kërkon një rrugë për një destinacion, ajo inicon një proçes rutim-zbulimi brenda rrjetit. AODV, DSR si dhe disa protokolle të reja bëjnë pjesë në këtë grup protokollesh.

1. **AODV (Ad Hoc On-Demand Distance Vector Routing)-** AODV është një përmirësim i protokollit DSDV. Nyjet që nuk ndodhen në rrugën e përzgjedhur nuk përmbajnë informacionin e rutimit ose marrin pjesë në shkëmbimet e tabele- rutimit. (E.Royer,Ch.K.Toh, Aprile 1999).

AODV përdor destinacionin e numrave të renditur(sekuencës) për të siguruar se të gjitha rrugët janë loop-free dhe të përmbajë informacionin më të fundit të ruterit. Dy aktivitet e rëndësishme të këtij protokolli janë:

– Zbulim Rrugëtimi - kryhet sa herë që një nyje ka nevojë për një "hop tjetër" për të përcjellë një paketë në një destinacion
– Mirëmbajtje e Rrugëtimit - Përdoret kur shkëputet linku, duke e bërë hop_in tjetër të papërdorshëm

Nëse një nyje- burim lëviz, kjo shkakton ri-inicializimin e protokollit te rutimit për gjetje zbulim- rrugëtim, pra për të gjetur një ruter te ri për në destinacion. Nëse një nyje lëviz përgjatë rrugës, fqinji i saj në rrjedhën e sipërme jep masën- njoftime dhe propagandon ose i shpërndan nje mesazh dështim-linku secilit prej fqinjëve të saj me aktive(afërt) për ta informuar atë për fshirjen e asaj pjese të kursit.

Mekanizmi Zbulim -Rrugëtim është i përdorur për të gjetur një rrugë drejt një destinacioni. Kurdo që një nyje gjeneron një pako, ajo kontrollon nëse ajo ka një rrugë të vlefshme për destinacionin e vet. Nëse nuk ndodh kështu, ajo transmeton një mesazh kërkesë – rrugëtim (RREQ) që do të marrë nga të gjitha terminalet që janë fizikisht më afër me të. Ndodhin tri situata kur një RREQ është pranuar: (1) nyja është vetë destinacioni dhe do përgjigjet me nje mesazh përgjigje- rrugëtim (RREP), (2) Nyja e kishte përpunuar tashmë një tjetër RREQ me të njëjtin çift nyjesh objektiv- burim si identifikim unik; (3) nyja shton adresën e saj më pas ritransmeton RREQ. Siç mund të shihet, kur RREQ arrin nyjen e synuar, ajo ka informacion në lidhje me të gjitha nyjet e vizituar gjatë rrugës drejt destinacionit.

Route Request (RREQ) - kërkesë rrugëtimi/kurs

Route Reply (RREP) - përgjigje rrugëtimi/kurs

Processing a RREQ Message:

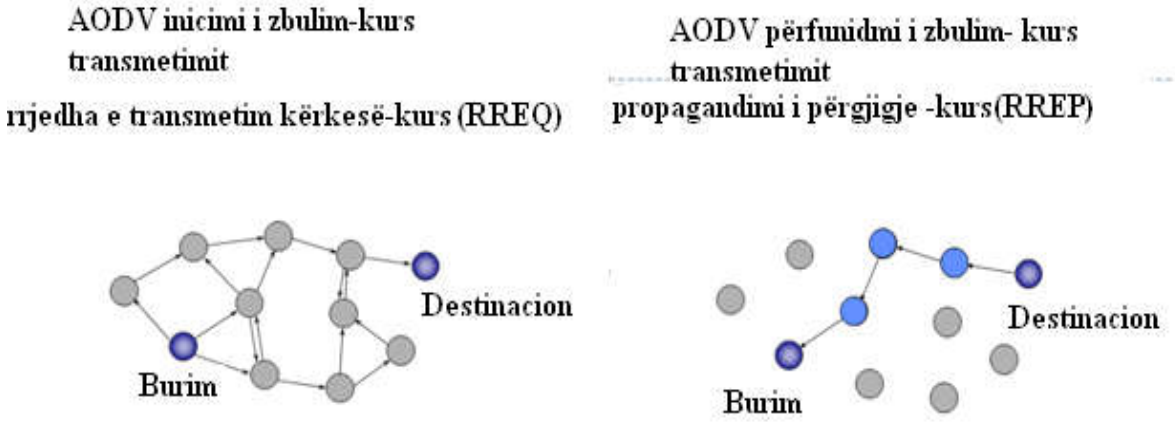


Figura 3.10 Mekanizmi Zbulim -Rrugëtim

- <ID- transmetimi, IP- adresa > çift i burimit S formon një identifikues unik për RREQ. Supozoni një nyje N që merr RREQ nga S. N kontrollon së pari nëse ajo ka marrë këtë RREQ më parë. Secila nyje magazinon çiftet< ID- transmetimi, IP- adresa > për të gjithë RREQ_tet e fundit që ajo ka marrë. Nëse N e ka parë këtë RREQ nga S tashmë, N discards RREQ. Përndryshe, N përpunon RREQ: N krijon një hyrje të kundërt të kursit në tabelën e saj të rrugëtimit për burimin S. Kjo hyrje përmban adresën IP dhe numrin aktual sekuencial të S, numrin e hops në S dhe adresën e fqinjit prej të cilit N mori edhe RREQ.

Tre gjëndje të rëndësishme:

Unicasting

- AODV është rrugëtimi pikë-me-pikë, kur një nyjë burim dëshiron të dërgojë një mesazh në një nyje destinacion.

Multicasting

- Në këto situata, një nyje dëshiron të dërgojë një mesazh në një grup nyjesh në rrjet. Ky quhet multicasting dhe grupi quhet një grup multicast.

Broadcasting

- Broadcasting/Transmetimi është një rast i veçantë i multicasting kur të gjitha nyjet në rrjet janë në grupin multicast.

AODV mbështet multicasting dhe unicasting brenda një kuadri uniform. Madhësia paketë në AODV është uniforme ndryshe nga DSR. Ndryshe nga AODV, DSDV nuk ka nevojë për transmetime të gjerë të sistemit për shkak të ndryshimeve lokale.

Ne mund përmbledhim se:

- Kërkesë-rrugëtimi (RREQ) përfshin numrin rendor të fundit të njohur për destinacionin
- një nyjë e ndërmjetme mund të dërgojë një rrugë Përgjigje- rrugëtimi (RREP) me kusht ose duke siguruar që ajo e di një rrugë më të fundit se ajo e njohur më parë për te dërguesi.
- nyjet e ndërmjetme që përcjellin RREP, gjithashtu regjistrojnë hop_in tjetër në destinacion
- një tabelë- kurs që hyn duke mbajtur një rrugë të kundërt, shlyhet pas një kohe jashtë intervalit.

2. DSR(Dynamic Source Routing) është një protokoll rutimi për rrjetat MESH wireless**.** DSR**-** është bazuar në konceptin e rutimit burim. Nyjet në lëvizje ngarkohen të kenë një memorje të vogël por të shpejtë, tip memorje cashe[40], të cilat mbajnë kursin e burimit pë të cilat lëvizja është e vetdijshme. Përmbajtja e cashes update$_{\text{-ohet}}$ vazhdimisht sa herë që një kursi I ri mësohet. Dhe në fakt ky protokoll përmban dy faza(E.Royer,Ch.K.Toh, Aprile 1999):

a. Zbulimi i rutimit(kursit)
b. Mirëmbajtja e rutimit.

Kështu kur një nyje e lëvizshme ka një paketë për të dërguar në destinacion, së pari konsulton cashe$_{\text{_n}}$ rutimi për të përcaktuar se kur mund të disponojë nje kurs(rutim) për në destinacion. Në të kundërt nëse nyja nuk ka një ruter të disponueshëm inicalizohet faza e kërkimit ose zbulimit të rutimit duke broadcasting një paketë kërkesë – rutimi, që përmbajnë adresën e destinacionit, bashkë me adresën e nyjeve burim dhe një numër unik identifikues. Secila nyje që merr paketën kontrollon njëherë nese ajo e njeh këtë rrugë për në destinacion. Kur është negative, pra nuk e njeh, ajo shton adresën e vet në rekordin-

[40] Memorje e vogël e shpejtë, pjesë e memorjes qëndrore

rutimit të paketës, përcjell paketën përgjatë linkut të daljes. Një përgjigje rutimi (ruter replay) gjenerohet kur kërkesa për rutim arrin në destinacionin e vet ose nyjen që përmban cashe me rekordin- rutim që lëshon skuencat e marra Hops. *Mirëmbajtja e rrugëtimit* realizohet nëpermjet përdorimit të paketave gabim-rutimi dhe pranimeve (acknowledgments) ose njohjet që përdoren për të verifikuar operacionet e rregullta të linke_ve kurs. Pako gabimit rrugë janë të krijuara në një nyje kur shtresa Lidhje të dhënave ballafaqohet me një problem fatal të transmetimit. Kur një paketë me gabim-rrugëzimi është pranuar, hop_i në gabim ka larguar nga rruga cache nyjen dhe të gjitha rrugët që përmbajnë hop janë cunguar në atë pikë. Përveç mesazhet e gabim- rrugëzimit, mirëmbajtja është përdorur për të verifikuar funksionimin korrekt të lidhjeve rrugës. Njohuri të tilla përfshijnë mirënjohje pasive, ku një celular është në gjendje të dëgjojnë hop tjetër duke forwarding paketën përgjatë rrugës.

3. TORA (Temporally Ordered Routing Algorithm) - shpikur nga Vincent Park dhe M.Scott Corson nga Universiteti i Marylandit. Tora është një protokoll rutimi on-demand.

• Objektivi kryesor i Tora është të limitohet përhapja e mesazh- kontrollit në mjedis dinamik mobile.

• Çdo nyjë duhet të iniciojë një query kur i nevojitet dërgimi i të dhënave në një destinacion të veçantë

Tora kryen tri detyra(E.Royer,Ch.K.Toh, Aprile 1999):

- Krijimi i një routeri nga burimi në destinacion
- Mirëmbajtja e ruterit
- Fshirja e ruterit kur rruga nuk është më e vlefshme

Tora tenton të ndërtojë atë që është i njohur me grafi i drejtuar aciklik(DAG) i cili është i ingranuar në destinacion.

Ideja është së pari të ndërtohet një DAG nga burimi në destinacion dhe pastaj nëse kemi dështim linkesh, bëhet i nevojshëm rindërtimi i një DAG i tillë që të gjejë ruterin.

Në kohën e lëvizshmërisë nyjes DAG -kursi prishet, dhe për mirëmbajtjen e kursit e nevojshme të krijojet një DAG i ngulitur në të njëjtin destinacion. Siç është paraqitur në

Figurën 2.12. b(E.Royer,Ch.K.Toh, Aprile 1999), pas dështimit të lidhjes së fundit në drejtim të rrymës, një nyje gjeneron një nivel të ri referimi që rezulton në propagandimin e këtij niveli të referencës nga nyjet fqinje, duke koordinuar në mënyrë efektive një reagim të strukturuar ndaj dështimit.

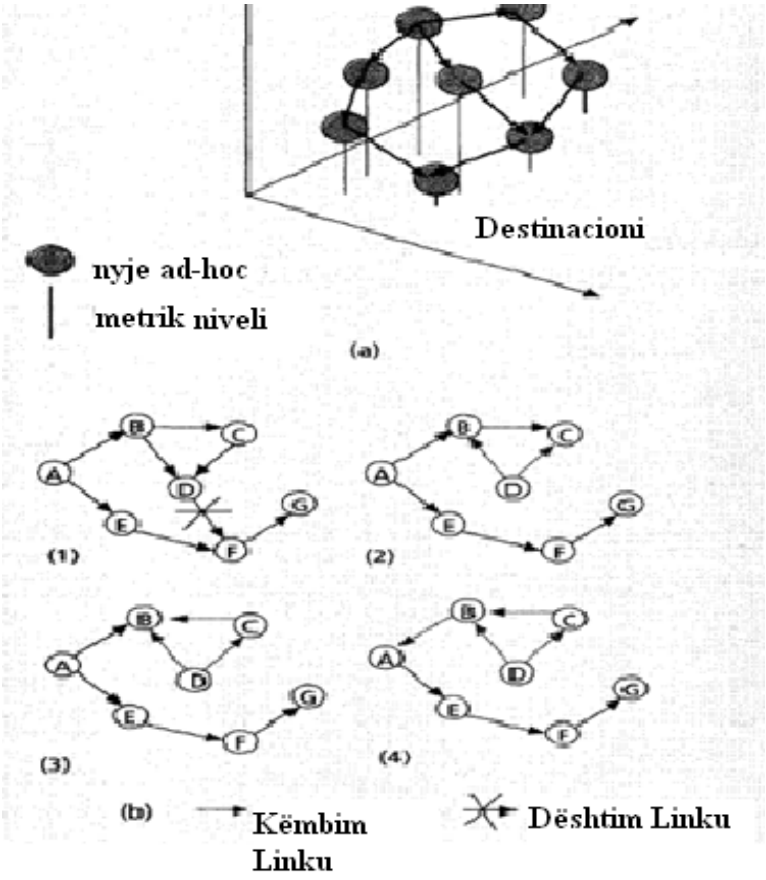


Figura 3.11 a) Krijim- rutimi në TORA; b) Mirëmbajtje-rutimi në TORA

Metrikë i Tora është një pesëfish i përbërë nga pesë elemente, të emërtuar:

1. Koha logjike e një dështim-Linku
2. ID unike e nyjës që përcakton referenca e re
3. Një bit tregues reflektimi
4. Një parametër urdhër- përhapje/propagandimi
5. ID unike e nyjes

Tre elementët e parë së bashku përfaqësojnë nivelin e referencës. Një nivel i ri i referencës është përcaktuar sa herë që një nyje humbet lidhjen e tij të fundit në drejtim të rrymës për shkak të dështim- link_ut. (E.Royer,Ch.K.Toh, Aprile 1999). Faza fshirje -rrugës në Tora në thelb përfshin përmbytjet e një pakete qartë e transmetuar (CLR) në të gjithë rrjetin për të fshirë rrugët e pavlefshme.

Pra TORA përdor koordinim ndërnyj_or, paqëndrushmëria e problemit të tij është e ngjashme me "të numëruarit-deri-në pafundësi " problem ky në protokollet e rutimit distancë-vektor, përveç se duhet thënë se luhatje të tilla janë të përkohshme dhe konvergjenca- kurs do të ndodhë në fund të fundit.

ABR(Associativity-Based Routing) – ABR është një kompromis midis rutim-transmetimit dhe atij të dyanshme [point-to-point]. ABR siguron rrugëtimin vetëm për ato burime që e dëshirojnë një gjë të tillë. Por ABR nuk ka funksionin e rindërtimit të rrugëtimit mbi bazën e informacionit për rrugët alternative, të depozituar në IN-të (duke mënjanuar kështu rrugët e konsumuara). Veç kësaj, vendimet e rrugëtimit performohen në DEST ku vetëm rruga më e mirë zgjidhet e përdoret ndërsa të gjitha rrugët e tjera të mundshme mbeten pasive, gjë që shmang duplikimin e paketës. Gjithashtu, për shkak të cilësisë së bashkëshoqërimit/ ndërlidhjes, siç përshkruhet më poshtë, rruga e zgjedhur ka gjasa të jetë më jetëgjatë. Ndonëse protokolli ABR nuk është projektuar për të mbështetur garancitë e QoS-it, protokolli ynë i ABR-së megjithatë i dallon cilësisht rrugët e mundshme. Rrjedhimisht, krahas mbështetjes së aplikimeve bashkëpunues, ABR mund të përdoret për të mbështetur edhe aplikimet multimediale adaptive të lëvizshme. (Sugikawa, Y. Morioka, K. Iwamura, Y. Tajika and M. Nakamura April 1995)

Në të dallohen qart tri faza:

- Zbulim kursi
- Rindërtimi i kursit(RRC)
- Fshirja e kursit

Faza zbulim- kursi është kryer nga një query transmetimi dhe një cikli ‘presë-përgjigje’ (BQ-REPLY). Një nyjë që dëshiron një rrugë transmeton një mesazh BQ në kërkim të

mobile_ve që kanë një kurs për në destinacion Të gjitha nyjet që marrin këtë query (që nuk janë destinacioni) ia bashkëngjitin adresat e tyre dhe ticks[41] shoqëruese fqinjëve të tyre, së bashku me informacionin e QoS së paketës query. Një nyjë pasardhëse fshin hyrjet tik shoqeruese të fqinjëve në rrjedhën e sipërme të saj dhe ruan vetëm hyrjen që ka lidhje me të dhe nyjen e saj në rrjedhën e sipërme. Në këtë mënyrë, çdo paketes rezultante që mbërrin deri në destinacion do të përmbajë ticks shoqëruese të nyjeve përgjatë rrugës për në destinacion. Destinacioni është në gjendje për të zgjedhur rrugën më të mirë duke ekzaminuar ticks shoqëruese përgjatë secilës prej rrugëve. RRC mund të përbëhet nga zbulimi i pjesshëm i rrugës, fshirja e rrugës së pavlefshme, përditësimet e rrugës së vlefshme, dhe zbulim i rrugës së re, në varësi të rrugës përgjatë së cilës nyja (s)lëviz. Kur një rrugë e zbuluar nuk dëshirohet, nyja burim fillon një transmetim fshi-kurs(rout – deleted/RD) në mënyrë që të gjitha nyjet përgjatë rrugës të update_ojnë tabelat e tyre të rutimit. Mesazhi RD është përhapur nga një transmetim i plotë, në krahasim me një transmetim të drejtuar, sepse nyja burim nuk mund të jetë në dijeni të ndonjë ndryshim të rrugës së nyjes që kanë ndodhur gjatë RRC.

4. **SSR (Signal Stability Routing):** Ky është një tjetër protokoll që bënë pjesë në protokollet on-demand. Ndryshe nga algoritmet e përshkruara deri më tani, SSR zgjedh rrugët e bazuar në fuqinë e sinjalit ndërmjet nyjeve dhe stabilitetit të vendodhjes lokacionit së një nyje. Ky kriter përzgjedhje- rrugëzimi ka efektin e zgjedhjes të rrugëve që kanë lidhje "të fortë". SSR mund të ndahet në dy protokolleve të bashkëpunimit: Dynamic Routing Protocol (DRP) dhe Static Routing Protocol(SRP). Ku DRP është përgjegjës për mirëmbajtjen e Tabelës së Stabilitetit të Sinjalit (SST) dhe Tabelës së Rutimit (RT). SST regjistron fuqinë e sinjalit të nyjeve fqinje, e cila është marrë nga sinjalizuesit periodike nga shtresa link e çdo nyje fqinje. Fuqia e sinjalit mund të regjistrohet si një kanal i fortë apo i dobët. Të gjitha transmetimet janë marrë nga, dhe të përpunuara në DRP. Pas përditësimit të të gjitha hyrjeve të nevojshme tabelë, DRP kalon një paketë të marrë në SRP. Të SRP përpunon paketat duke kaluar paketën gjer në grumbullim, nëse është marrësi i synuar apo në kërkim deri në destinacion në RT dhe

[41] Tik-tak/tike

pastaj e përcjell paketën në qoftë se nuk është e duhura. Nëse nuk ka hyrje në RT për destinacionin, një proçes rrugë-kërkimi është iniciuar për të gjetur rrugën. Kërkesat për rrugë propagandohen në të gjithë rrjetin, por janë dërguar vetëm për hop_in tjetër në qoftë se ata janë pranuar mbi kanale të forta dhe nuk janë përpunuar më parë (për të parandaluar krijim laku/looping).

3.2 Krahasimi Mes Protokolleve Të Rutimit Për Rrjetet Ad – Hoc Wireless

Më poshtë do të jepet një krahasim midis të gjithë këtyre protokolleve që u përmendën më lartë për rrjetet ad-hoc wireless.

Për protokollet e rutimit Table-driven, ky krahasim do fillojë të paraqitet me anë të një tabele të dhënë më poshtë **(**E.Royer, Ch.K.Toh, Aprile 1999)

Tabela 3.2. Krahasimi ndërmjet protokolleve të rutimit Table-driven

Parametrat	**DSDV**	**CGSR**	**WRP**
Kompleksiteti Kohë / (shtesë linku/dështim)	**O(*d*)**	**O(*d*)**	**O(*h*)**
Kompleksiteti i komunikimit/ (shtesë linku/dështim)	**O(x=N)**	**O(x=N)**	**O(x=N)**
Filozofia e rutimit	**I rrafshët**	**Hierarkik**	**I rrafshët***
Cikël i Lirë(loop free)	***Po***	***Po***	***Po(por jo i menjëhershëm)***
Aftësi Multicast	***Jo***	***Jo****	***Jo***
Numri i tabelave të kërkuara	**2**	**2**	**4**
Frekuenca e Transmetimeve të përditësuara	**Periodikisht dhe sipas nevojës**	**Periodikisht**	**Periodikisht dhe sipas nevojës**
Përditësimet Transmetohen në	**Fqinjët**	**Fqinjët dhe kreu-**	**Fqinjët**

		grup(claster head)	
Shfrytëzon numrat sekuencial	***Po***	***Po***	***Po***
Shfrytëzon mesazhet hello	***Po***	***Jo***	***Po***
Nyjet kritike	***Jo***	***Po(cluster head)***	***Jo***
Metrikë rutimi	***Rruga më e shkurtër(shortes path)***	***Rruga më e shkurtër***	***Rruga më e shkurtër***
Shkurtime: **N= numri i nyjeve në rrjet** **d= diametri i rrjetit** **h= Lartësia e pemës kurs** **x= Numri i nyjeve të ndikuar nga një ndryshim topologjik** *** Ndërsa WRP përdor adresimin e sheshtë, ajo mund të përdoret në mënyrë hierarkike** **** Vetë Protokolli momentalisht nuk e mbështet multicast; Megjithatë, ekziston një protokoll i veçantë, i cili shkon në krye të CGSR dhe siguron aftësi multicast**			

Përveç krahasimit tabelor, i cili na jep dijeni mbi performancën dhe disa elemente të protokolleve të rutimit Table-driven, mund të shtojmë në vazhdimësi për secilin prej tyre se:

DSDV: kërkon një up-to- date të rregullt të tabelës së rutimit, përdor të gjithë fuqinë e baterisë si dhe një sasi të vogël të 'bandwidth' edhe kur rrjeti është bosh ose jo i ngarkuar. Topologjia e rrjetit ndryshon dhe një sekuenë numerike e re është e nevojshme para se rrjeti të ri-konvergjjë. Ky protokoll nuk është i përshtatshëm për rrjetat me dinamikë të lartë. Stabiliteti dhe shkallëzueshmëria e DSDV garanton rutime me cikël-të lirë në paketat kurs. Ai përdor shuarje të plota dhe në rritje për përditësime. Përditësimi rritës është përdorur në mënyrë që e gjithë tabela kurs të mos ketë nevojë që të transmetohet për çdo ndryshim në toplogjinë e rrjetit. Gjithësesi, DSDV kërkon periodikisht update të shuarjes se plote, pavarësisht nga numri i ndryshimeve në topologjinë e rrjetit. Në këtë aspekt, DSDV nuk është efikas në update_imin e rrugëtimit/kursit.

CGSR: ngjason me protokollin DSDV, vetëm se këtu nevojiten 'cluster- heads' and 'gateways'(portat). Një avantazh i këtij protokolli është që mund të përdoren disa metoda heuristike për të përmirësuar performancën e protokollit.

WRP: ky protokoll ndryshon në disa pika nga protokollet e sipër përmendura. Së pari ky protokoll kërkon që çdo nyje të mbaje katër tabela rutimi. Kjo mund të çojë në kërkesa sinjifikante, reale të memorjes, sidomos kur numri i nyjeve në rrjet është i madh. Gjithashtu ky protokoll kërkon përdorimin e paketave hello sa herë që nuk ka transmetime recente të paketës nga një nyje e caktuar. Ky protokoll bënë pjesë në klasën e algoritmave gjetje-path_i (path –finding), por ky si protokoll ka një avantazh, ai shmang problemin e krijimit të cikleve (loops) të rutimit të përkohshëm që këto algoritma kanë gjatë verifikimit të informacionit parardhës. Ka kompleksitet kohe më të ulët sesa DSDV.

Pasi krahasuam me rradhë të gjithë protokollet e rutimit Table-driven, po nisim me krahasimin e protokolleve të rutimit *Source –Initiated On –Demand:*. Edhe këtë krahasim do ta nisim me ilustrimet dhe krahasimin e parametrave të paraqitur në tabelën e më poshtme të modeluar dhe sqaruar tek **(**E.Royer, Ch.K.Toh, Aprile 1999).

Tabela 3.3 Krahasimi ndërmjet protokolleve të rutimit source-initiated on-demand

Performanca e Parametave	**AODV**	**DSR**	**TORA**	**ABR**	**SSR**
Kompleksiteti Kohë (inicializimi)	***O(2d)***	***O(2d)***	***O(2d)***	***O(d+z)***	***O(d+z)***
Kompleksiteti Kohë (pasdështim)	***O(2d)***	***O(2d)ose 0****	***O(2d)***	***O(d+j)***	***O(d+j)***
Kompleksiteti Komunikimi (inicializimi)	***O(2N)***	***O(2N)***	***O(2N)***	***O(N+y)***	***O(N+Y)***
Kompleksiteti Komunikimi	***O(2N)***	***O(2N)***	***O(2x)***	***O(x+y)***	***O(x+Y)***

(pasdështim)					
Filozofia e rutimit	***I rrafshët***	***I rrafshët***	***I rrafshët***	***I rrafshët***	***I rrafshët***
Cikël/Lak-Lirë (loop-free)	***Po***	***Po***	***Po***	***Po***	***Po***
Aftësi Multicast	***Po***	***Jo****	***Jo***	***Jo***	***Jo***
Kërkesa sinjalizuese	***Jo***	***Jo***	***Jo***	***Po***	***Po***
Mundësi për rutim të shumëfishtë	***Jo***	***Po***	***Po***	***Jo***	***Jo***
Rutimi i mbajtur në:	***Tabelë-Rutimi***	***Cache-Rutimi***	***Tabelë-Rutimi***	***Tabelë-Rutimi***	***Tabelë-Rutimi***
Përdor cache të rutimit / Kohëmatës i skadimit të tabelës	***Po***	***Jo***	***Jo***	***Jo***	***Jo***
Metodologjia e konfigurimit të rutimit	***Fshi rutim / Njofto burim***	***Fshi rutim / Njofto burim***	***Pezullim Linku/ Riparm rutimi***	***Lokalizim i quer_it të transmetimit***	***Fshi rutim / Njofto burim***
Metrika të Rutimit	***Rruga më e freskët dhe më e shkurtër***	***Rruga më e shkurtër***	***Rruga më e shkurtër***	***Shoqërizimi dhe rruga e shkurtër dhe te tjera******	***Shoqërizimi dhe Stabiliteti***

Shkurtime:

l= diametri i segmentit të prekur të rrjetit

y= numri totatl i nyjeve që formojnë pathin e drejtuar ku paketa REPLY kalon

z= diametri i pathit të drejtuar ku paketa REPLY kalon

***cache qëllon/arrin sukses**

****ashtu si CGSR edhe TORA gjithashtu nuk e mbështet multicast, megjithatë është një protokoll i**

veçantë, LAM, i cili vepron në krye te TORA dhe i siguron mundësi multicast.
ABR- gjithashtu përdor rutimin duke zhvilluar sërisht(replaying) ngarkesën dhe vonesat kumulative përcjellëse si metrika te rutimit.

- AODV i nevojitet një numër shumë më i vogël paketash overhead[42], krahasuar me DSDV.
- Paketat e overhead në AODV janë si pasojë e mesazheve RREQ, RREP dhe RERR.
- Numri i paketave overhead rritet me rritjen e lëvizshmërisë, duke qenë se kjo e fundit shkakton rënie të shpeshta linje dhe gjetje rrugësh.
- Vonesa në gjetjen e rrugëve në AODV është më e vogël krahasuar me DSR dhe DSDV.
- Vonesa është thuajse e pandryshueshme edhe me rritjen e lëvizshmërisë nëse përqendrimi i nyjeve [nodes] mbetet i ngjashëm.
- Gjatësia mesatare e path_it për gjetjen e rrugëve është po ashtu mjaft e ulët.
- DSR, AODV janë të ngjashme në fuqinë e përcjelljes së paketave.
- DSR ka harxhim shumë më të ulët trafik rrugësh transmetimi [routing] (përjashtuar zgjatimin e rrugëve të transmetimit të DSR-së në çdo paketë të dhënash).

Dobësitë tek protokolli AODV vërehen tek:

- Latenca
- Transmetime të Zbulim-rrugëzimit
- ICMP i pakapshëm vetëm pas përpjekjes për zbulim-rrugëzimi

[42] të ngarkuara

Përsa i përket konvergjencës së Performancës:

- Konvergjenca është aftësia e protokollit të rutimit për të "stabilizuar" me shpejtësi rrugët që njeh.
- DSR & AODV gjithmonë përcjellin të paktën 95% të paketave të dërguara në çdo rast.
- TORA nuk arrin të konvergjojë në më pak se ~500s kohë pushimi por gjithmonë konvergjon për 10 dhe 20 burime.
  - Krijohet Lak/Cikël për shkak të ngjeshjes/mbipopullimit
- DSDV nuk konvergjon me kohë pushimi më të ulët se ~300s kur nyjet lëvizin me shpejtësi 20 m/s.

3.3 Paraqitja e Performancës me Dy Simulator, MATLAB dhe DARS.

3.3.1 Implementimi dhe Performanca e Protokollit AODV me anë të simulimeve në MATLAB simulator.

Efektiviteti i komunikimit navigacional rritet duke optimizuar parametrat e protokollit AODV per rrjetat e lëvizshme ad-hoc wireless. Sigurisht shihet paraqitja e efiçencës më të mirë, për një numër të caktuar nyjesh, deri në pikën optimale.

SIMULIMI: Si simulator është përdorur MATLAB për algoritmin e rutimit AODV, për karakteristikat e të cilit kemi folur në paragrafët më sipër. Si metrik, zakonisht në rrjetat ad hoc wireless, për këto lloj protokollesh përdoret '*numri i hopeve për në destinacion'*

Kodi për performancën (implementation and Source code in MATLAB, by Rupam):

```
function [thrput]=performance(packet_total,node,dist,Max)
 r=randperm(100);
d=dist;
% per packet transmission watt energy loss.threashold 20% of original.
for j=1:1:length(node)-1
n1.es=node(j).es;
n2.es=node(j+1).es;
```

```
 threashold=n1.es*.2
packetsent=0;
eloss=d*.01;
  % each packet looses .01 watt energy%
while(n1.es> threashold)
   n1.es=n1.es-eloss;
   node(j).es=n1.es;
  if(packetsent<packet_total)
    packetsent=packetsent+1;
  end
end
```

Kodi për lëvizjen e nyjeve, hopet në destinacion:

```
 clc;
clear all;
Max=10;
for(i=1:1:Max)
n(i,:)=randint(1,2,[2 100])
end
%n(2,:)=randint(1,2,[2 100])
%n(3,:)=randint(1,2,[2 100])
%n(4,:)=randint(1,2,[2 100])
%n(5,:)=randint(1,2,[2 100])
for i=1:1:Max
%stem( n(i,1),n(i,2))
plot( n(i,1), n(i,2),'--rs','LineWidth',2,...
                'MarkerEdgeColor','k',...
                'MarkerFaceColor','g',...
                'MarkerSize',10,...
                'Tag','hi')
```

```
hold on;
end
grid on;
hold on;
 % e RREQ të gjenerua
RREQ.Src=1
RREQ.Dst=5
 %%%%%%%% të gjitha nyjet gjenerojnë një paketë 'Hello' duke vënë kohën e fillimit
kur merren nga destinacioni koha është llogaritur dhe kjo distancë është marrë.
xs=0
ys=0
for i=1:1:Max
   for j=1:1:Max
      if(i==j)
      d(i,j)=0
      else
         xs=(n(i,1)-n(j,1))*(n(i,1)-n(j,1))
         ys=(n(i,2)-n(j,2))*(n(i,2)-n(j,2))
         d(i,j)=sqrt(xs+ys)
      end
         end
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
 path=RREQ.Src;
current=RREQ.Src;
INF=999999999999999
small=INF
```

```
tmp=0;
while current~=RREQ.Dst
      for i=1:1:Max
       if current~=i
         if( d(current,i)<small)
           k=ismember(path,i);
           k=find(k);
           if(k)
             disp 'hi'
           else
           small=d(current,i)
           tmp=i;
           end
         end
      end
  end
   current=tmp;
   path=[path current]
   small=INF
   end
disp 'loop ends'
path
 sz=size(path)
sz=sz(:,2)
x1=n(path(1),1)
rows=x1
   x2=n(path(1),2)
 col=x2
for i=2:1:sz
```

```
    x1=n(path(i),1)
 rows=[rows  ;x1]
    x2=n(path(i),2)
    col=[col;x2]
  end
 x=[rows col]
  plot(x(:,1),x(:,2))
   r=randperm(100);
  for j=1:1:4
    node(j).es=r(j);
 end
 A=[20,60,100,120,160,200,250,300]
  for i=1:1:8
   thrput(1,i)=performance(A(1,i),node,d,Max);
  end
 figure()
 plot(A, thrput)
```

Sipas këtij algoritmi:

- pasi vendoset vlera për variablin max (që nënkupton maksimumin e nr. të nyjeve),
- proçesohet një mesazh RREQ

  RREQ.Src- kërkesë burimi(request source)

  RREQ.Dst –kërkesë destinacioni (request destination)

- njihen fushat për RREQ:
- më pas të gjitha nyjet gjenerojnë një paketë 'Hello(Hi)'në kohën e startimit.
- kur merren nga destinacioni llogaritet koha, përftohet distanca.
- xs dhe ys, vlerat që do të mbajne këto dy variabla përfaqësojnë koordinatat e nyjes dhe ndihmojnë në llogaritjen e distancës 'd', d(i,j)= sqrt(xs+ys).

Tabela përmbledhës e paraqitur më poshtë paraqet dhe shpjegon disa parametra, që bëjnë pjesë në këtë algoritëm rutimi:

Tabela 3.4. Parametrat e Simulimit për protokollin AODV

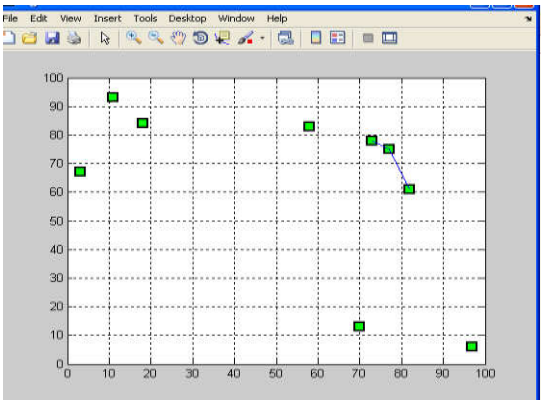
Parametrat e Simulimit	
Routimi	AODV
MATLAB	7.10.0(R2010a)
xs, ys	koordinatat per nyjen sipas boshteve
d-distanca	d(i,j)= sqrt(xs+ys)
A[ ]	[20,60,100,120,200,250,300]
Max(nr e nyjeve)	9, 10, 15, 20,,25,30,35,40,45,50,60,70, 80, 90
Hapsira e simulimit	100 x 100
Thrput	r=randperm(100)
Threshold	15

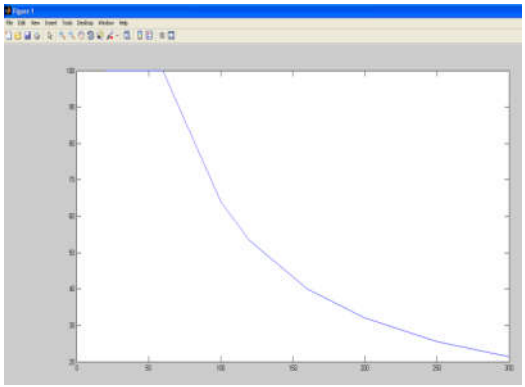
Më poshtë, nga 14 matjet e kryera janë paraqitur vetëm 4, mjaftueshëm për të parë sesi ndryshon performanca dhe koha me rritjen e nr. të nyjeve.

[throuput] = performance/xhirot

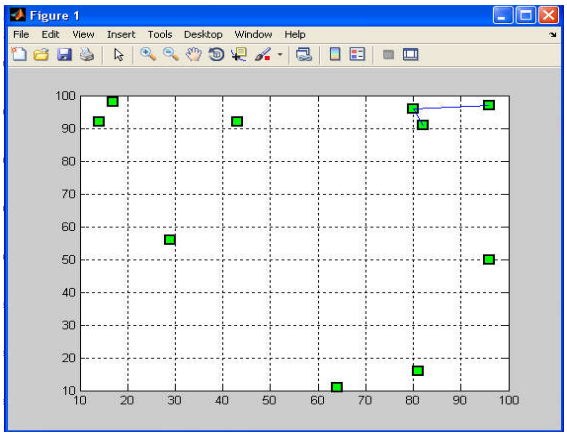
[threshold]= prag/kufi

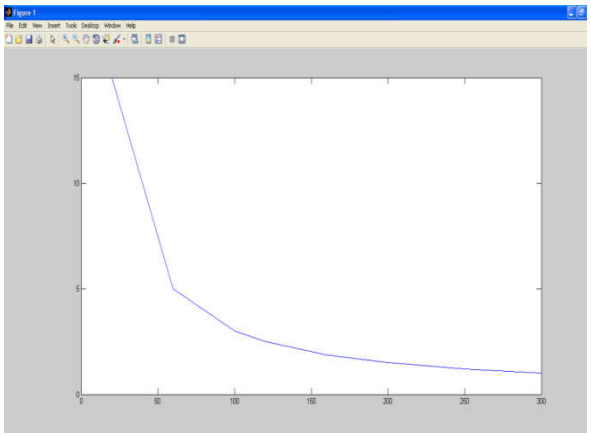
Matja 1: max= 9nyje, t = 2 sec - midis thruput dhe threshold



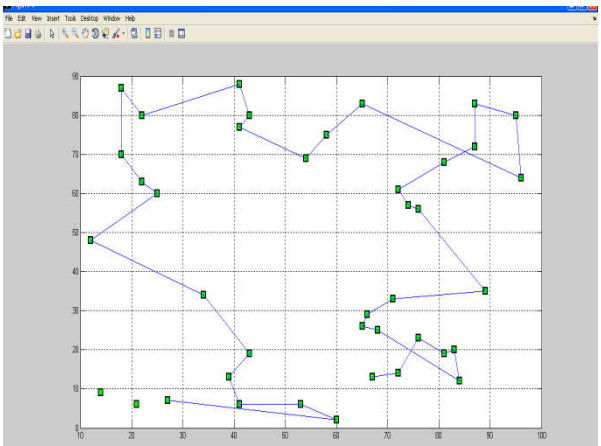


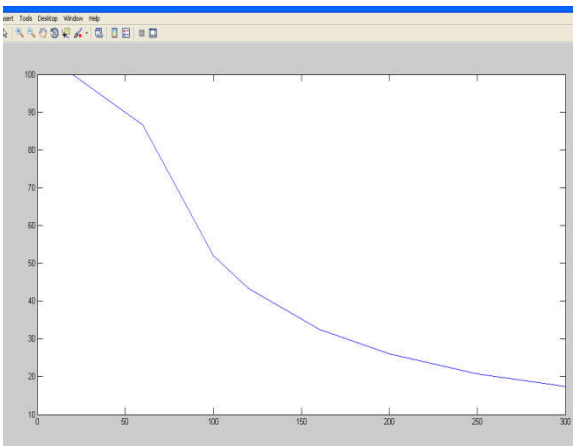
Matja 2: max= 10 nyje, t =30sec



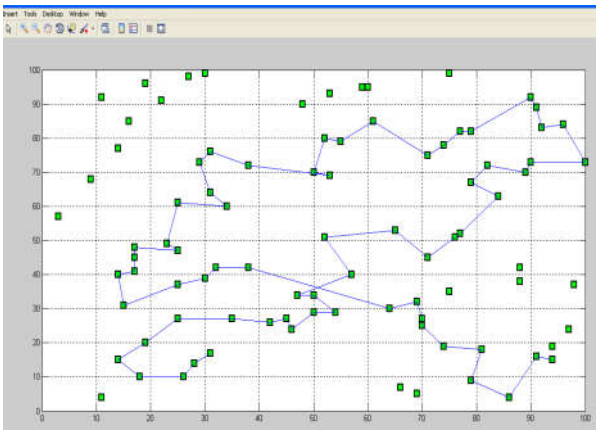


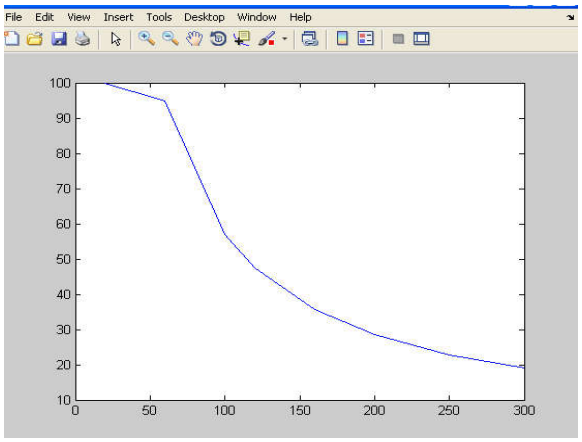
Matja e 7: max =50, t = 2min e 30 sec





Matja 12; max =90, t = 4min





Siç shihet me rritjen e numrit të nyjeve rritet edhe koha e performancës pra nga një thruput në një threshold dhe një numër i madh nyjesh nuk kanë një fqinjësi, ngelen të pambuluara. Deri tek matja 7 me max= 50 duket se është optimaliteti. Kjo dhe për faktin se n.q.s ne i referohemi metodologjisë kërkimore, paraqitur më lartë, për topologjinë e rrjetit, rrjeti ynë ka një topologji të rregullt kur max=50nyje.

Vërehet se për nr. nyjesh të =10 ose më të vogël se 10, sigurisht koha nga një thruput në një threshold është e vogël dhe topolgjia pak a shumë është e rregullt, por numri i nyjeve që nuk komunikojnë me njëra –tjetrën është më i madh ose mbulimi i rrjetit më i vogël.

2.3.3. Implementimi dhe Performanca e Protokollit AODV dhe DSDV me anë të simulimeve në DARS simulator

- DARS është projektuar për të lehtësuar kuptimin e Rrjetave Mobile Ad-hoc.
- I lejon përdoruesit të kryejnë skenare/plane të ndryshme, të zbatojnë protokolle të ndryshme të komunikimit dhe të studiojnë sjelljen e rrjetit.
- Ai shpjegon funksionimin e dy protokolleve të ndryshme AODV dhe DSDV në një mjedis miqësore dhe interaktive shumë përdorues.
- Simulatori jep të dyja edhe paraqitjen tekstuale dhe grafike të simulimit të rrugëtimit.
- Qëllimet kryesore të DARS konsistojnë në tre pjesë:
    1. Krijmin e një plani tërheqës dhe miqësor me përdoruesin.

2. Aftësinë për të aplikuar protokolle të ndryshme për një skenar/plan.
3. Mban/ruan gjurmët e ngjarjeve të rrjetit dhe t'i shfaq ato për përdoruesit.

DARS është projektuar të pranojë lehtësisht shtimin e protokolleve të reja te rutimit.

Shtimi i një protokolli mund të ndahet në tre hapa të mëdha:

- Freskimi i NodeFactory
- Zgjerimi i Klasës së Nyjeve
- Krijimi i një Kutize Dialogu të Protokollit

Freskimi i NodeFactory

- Fresko dars/proto/NodeFactory.java

Hapi 1: Shto një deklaratë të importit për klasë të re protokolli

import dars.proto.newproto.NewProto;

Hapi 2: Shto emrin e protokollit në renditjen NodeType.

public enum NodeType f AODV, DSDV, NewProto g;

Hapi 3: Trajtohen kërkesat e reja te nyjes për llojin e ri të protokollit. Shto një case te deklarata e radhës. Rasti i ri duhet të thërrasi ndërtuesin për protokollin. Ndërtuesi duhet të pranojë një argument të vetëm të tipit atribut i Nyjes. Ky konstruktor kërkohet si pjesë e klasës bazë abstrakte të nyjes. rasti NewProtoName : kthe NewProto(na); ?

Zgjerimi i Klasës Nyje

Klasa Nyje kërkon që një protokoll i ri të zbatojë gjashtë funksione. Zbatimi i protokollit mund të mos thërras asnjë nga këto funksione. Këto funksione po i paraqesim më poshtë:

1. messageToNetwork - Ky funksion është përdorur për të kthyer një mesazh off, radhën e transmetimit të një nyje dhe do ta kthejë ate për motor simulimi për tu konsumuar.

2. messageToNode - Ky funksion është përdorur për të dhënë një mesazh në një nyje. Mesazhi do të vendoset në nyje të fituara nga radhë efektike, nyja është duke marrë mesazhin.
3. newNarrativeMessage - Dërgo mesazh përshkrues nga një nyje në një tjetër.
4. clockTick - Procesi i një përsëritje të kësaj nyje. Ky do të bëjë të gjithë përpunimin për interval kohor të një nyje.
5. getNodeDialog - Kthim i një JDialog që do të shfaqet nga GUI.
6. updateNodeDialog - Përditësimi i JDialog i kthyer më parë me informacionin e fundit për një nyje që do të tregohet tek GUI.

Krijimi i një Protocol Dialog Box

- Çdo protokoll duhet të sigurojë një dialog box[43] që mund të shfaqet tek përdoruesi, që tregonë informacion në lidhje me një nyje të caktuar tek përdoruesi.
- Ky dialog duhet të zgjerojë klasen standarde JDialog.
- Zbatimi dhe dizajni i Protocol Dialog box i është lënë zhvilluesit i cili po zbaton protokollin.

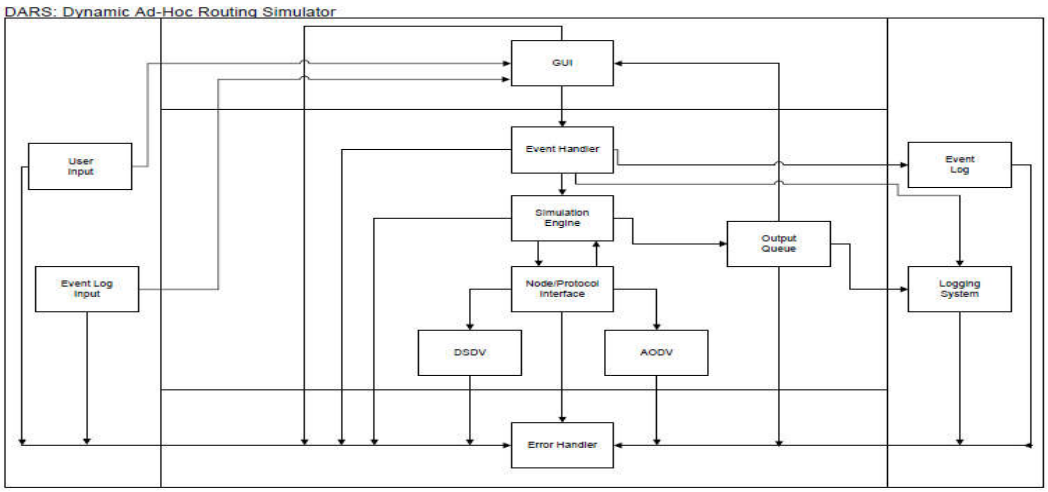


Figura 3.12. Arkitektura e DARS

[43] Kuti dialogu

Për të gjitha nyjet ne mund të marrin nga simulatori këto atribute: DEST,# HOPS, NXT HOP, SEQ#, INST TI.., siç tregohen edhe në figurën më poshtë:

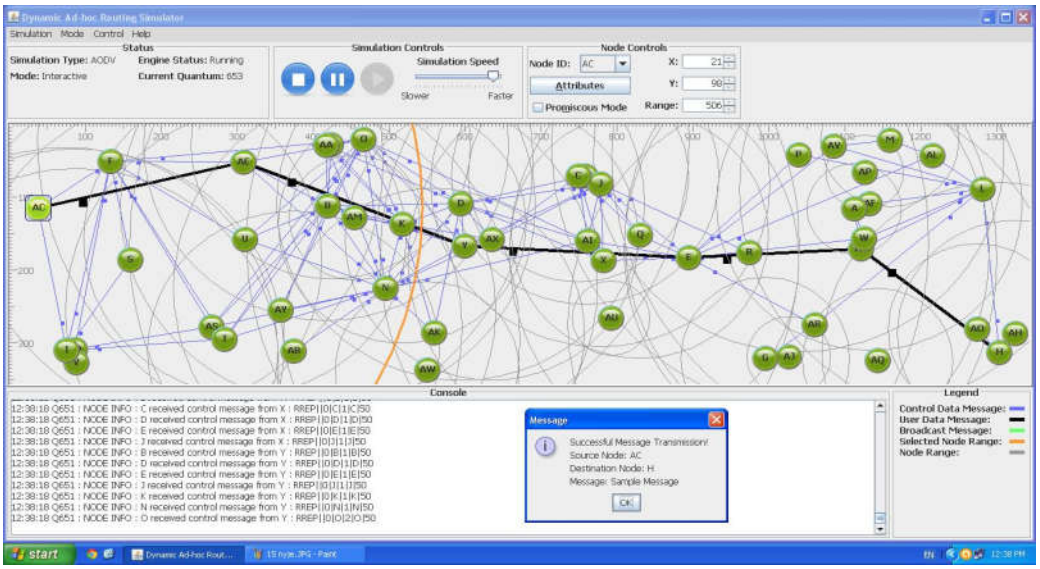
DEST	# HOPS	NXT HOP	SEQ #	INST TI...
AA	3	AQ	159	192
AB	4	AF	160	192
AC	4	AF	147	192
AD	3	AQ	141	192
AE	4	AF	170	192
AF	1	AF	169	192
AG	1	AG	127	192
AH	2	AQ	45	184
AI	2	BR	36	192

Figura 3.13 Parametra të Simulatorit

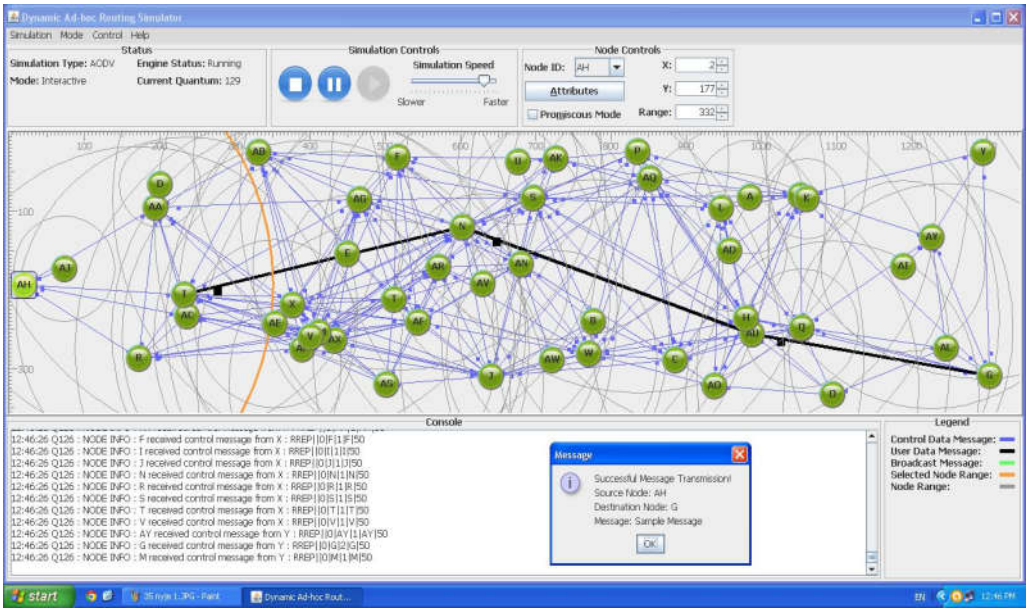
Matjet: Ndër matjet e kryera kemi paraqitur vetëm një pjesë prej tyre dhe për çdo matje është figura përkatëse. Matjet janë kryer për të dy protokollet AODV(Source –Initiated On –Demand) dhe DSDV (Table-Driven).

Matje 1. Numri i nyjeve = 15nyje, AODV

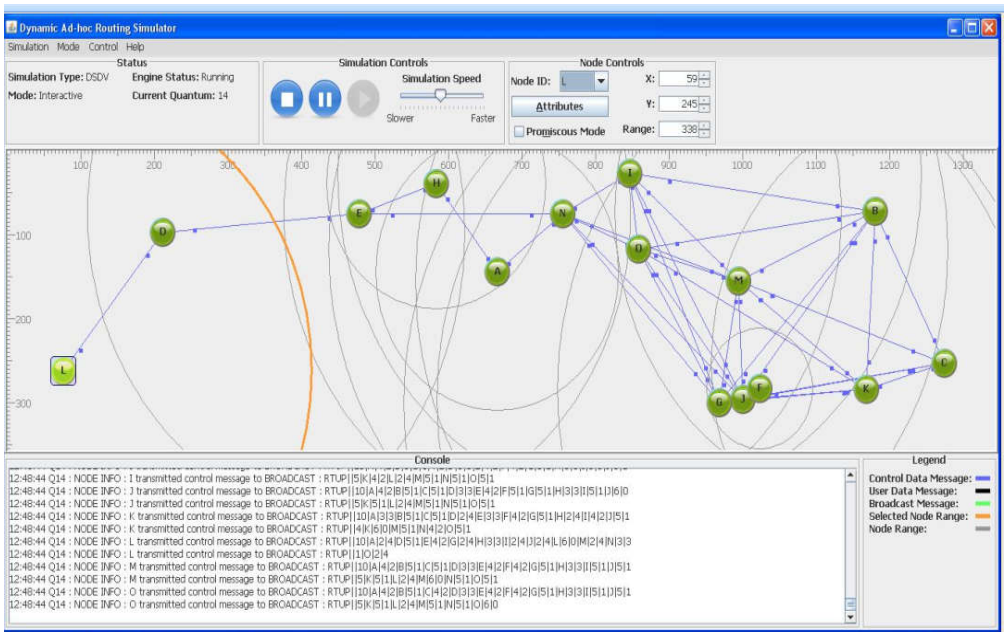
Matje 2. Numri i nyjeve = 35nyje, AODV



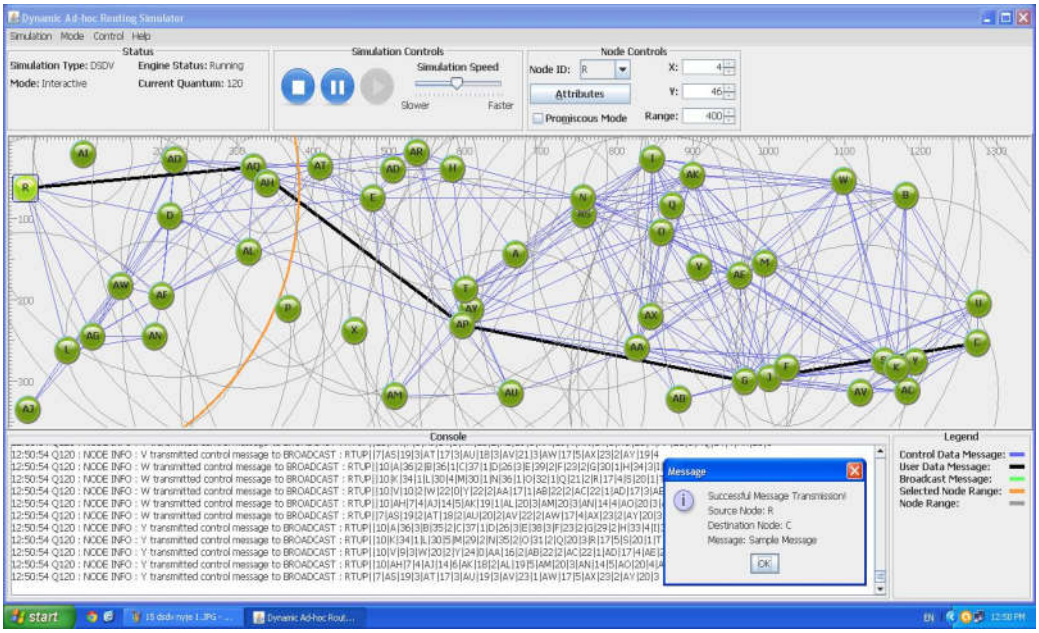
Matje 3. Numri i nyjeve = 50nyje, AODV



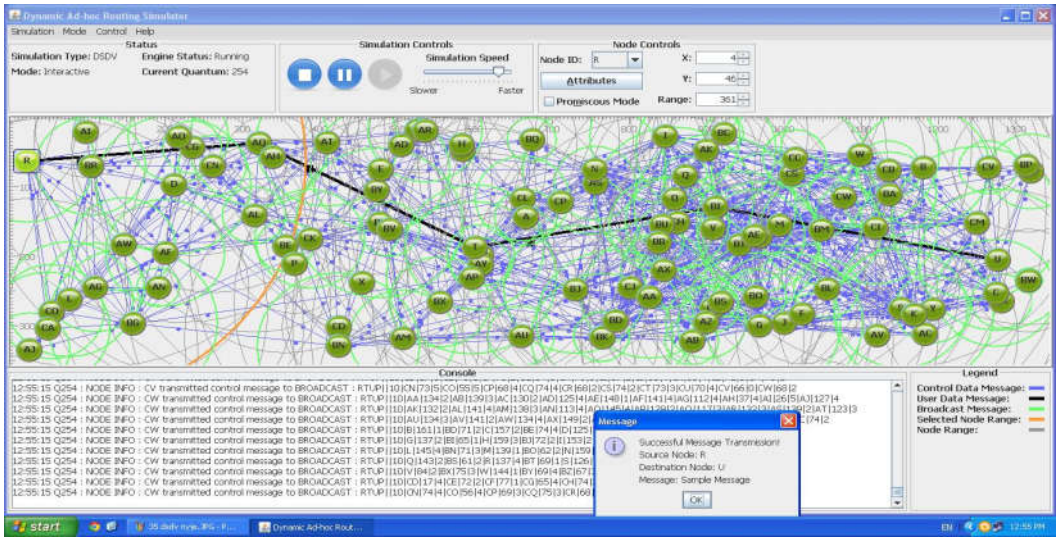
Matje 1. Numri i nyjeve = 15nyje, DSDV



Matje 2. Numri i nyjeve = 35nyje, DSDV



Matje 3. Numri i nyjeve = 50 node, DSDV



Gjatë këtyre simulimeve ne vërejtëm se kur numri i nyjeve rritej dhe në mënyrë konseguente distanca ndërmjet tyre ngushtohet kemi një përmirësim të komunikimit dhe një transmetim të sukseshëm të mesazhit.

3.4 Aplikueshmëria dhe Konkluzione

3.4.1 APLIKUESHMËRIA

Përparimi i shpejtë teknologjik në komunikimin e bazuar navigacional dhe hapsinor, kombinuar me karakteristikat rregullatore në rritje, si dhe presoni për të ulur sa më shumë rreziqet dhe koston përfaqësojnë mundësi të reja.

Niveli i lartë i sigurisë është një shqetësim i vazhdueshëm dhe në rritje. Aktiviteti detar i qëndrueshëm është vital për rritjen e sigurisë dhe ekonomisë botërore.

Duke u bazuar në karakteristikat e komunikimit mobile ad-hoc mund të themi se shërbimet e navigimit në rastet e emergjencës janë një aplikim i rëndësishëm i rrjeteve sensor dhe ad-hoc wireless për shpëtimin dhe sigurimin e jetës së njerëzve. Këto rrjete mund të gjejnë aplikueshmëri edhe në Shqipëri, me anë të protokolleve të përshtatshme rutimi mund të rritimin efektshërinë në komunikimin mjet me mjet dhe sidomos në komunikimet

navigacionale, p.sh anije me anije, ku ka nevojë për rrjetat wireless pa infrastrukturë mbështetëse.

Disa fusha ku mund të aplikohen këto protokolle:

- Ushtri – sistemet e luftimit, te mbikqyrjes(survejimit), zbulim.
- Menaxhimin e fatkeqesive
- Emergjencat mjeksore
- Navigim
- Edukim distance

Po kështu në këtë çështje u fol gjatë edhe për protokollin e rutimit AODV routing i cili është disenjuar për rrjetat mobile ad hoc wireless. Ky protokoll AODV mund të trajtojë norma të ulëta, të moderuara, dhe relativisht lëvizshmëri të lartë. AODV është projektuar për përdorim në rrjeta ku nyjet mund të besojnë njëri-tjetrit. AODV është disenjuar për të reduktuar përhapjen e kontrollit të trafikut dhe për të eleminuar të dhënat që e ngarkojnë trafikun

3.5 KONKLUZIONE

- Komunikimi efektive ndërmjet mjeteve rritet duke përdorur protokolle efektive rutimi.
- Një algoritëm i mirë rutimi mund të shmang bllokimin e trafikut mbi të gjitha linjat.
- Le të themi se rrjetat ad hoc janë të mirë- krijuar si një zonë praktike kërkimore. Kanë shumë aplikueshmëri.
- Një protokoll On-demand ofron shumë avantazhe
- AODV i përdor avantazhet si tek Distance-Vector dhe në On-demand
- AODV ka shance të mira për standartizimin.
- Rrjetat Ad hoc mund të vendosen në Internet dhe më pas të sigurojnë domain_et wireles. Teknikat e autokonfigurimit të addresave janë mirë-përshtatur.

KAPITULLI IV: PROPOZIMI I PROTOKOLLIT InterNavCom. SIMULIMET

4.1 Hyrje

Në këtë punim, ashtu siç theksuar edhe më parë, kemi menduar të prezantojmë një algoritëm rutimi, i cili merr në konsideratë problemet që lidhen me thithjen dhe shpërndarjen e mesazheve me anën e sinjaleve wireless, praninë e zonave 'gri', hazardet, në të cilat përjetohen pritje të rëndësishme, të ndryshueshme dhe të paqëndrueshme me kalimin e kohës dhe deri në rrezikun e dështimit të transmetimit. Ky algoritëm rutimi bazohet në një guidë të sigurtë për njerëzit për të realizuar një dalje të shpejtë nga zona e rrezik.

Kjo temë fokusohet në mundësimin dhe optimizmin e komunikimit ndërmjet nyjeve të një rrjeti ad-hoc që modelon rrjetin e komunikimit ndërmjet anijeve në port ose zonave përreth. Përdorimi i protokollit InterNavComm që merr në konsideratë të gjitha detajet specifike të komunikimit mes anijeve do të prezantojë një komunikim të shpejtë dhe efiçent.

Qëllimi *është që shpërndarja ose dorëzimi i mesazheve apo emergjencave të navigimit të bëhet në kohën e duhur, duke përdorur sa më pak burime te rrjetit dhe në kohën më të shkurtër të mundshme.*

Hipoteza: *Rritja e efektivitetit, disponibilitetit dhe sigurisë në protokollet ad-hoc inter-navale është një domosdoshmëri. Protokolli i ri InterNavComm është një protokoll i ri që siguron komunikim të vazhdueshëm dhe të sigurtë ndërmjet anijeve edhe në rastet e mungesës së infrastrukurës.*

Në portet shqiptare ngrihet nevoja e krijimit të aplikimeve të reja dhe të besueshme. Implementimi i protokollit InterNavComm edhe në portin e Vlorës do të ndihmonte në plotësimin e mangësive ekzistuese sidomos në zona me mungesë mbulimi valor.

Pyetja kërkimore: *Duke u nisur nga qëllimi që duam të arrijmë: A është me të vërtetë efiçent përdorimi i protokollit* InterNavComm *të rutimit për rrjetat ad-hoc wireless në navigacion, në komunikimin pikë më pikë/ anije me anije?*

- Si do të bëhet modelimi i rrjetit të kompjuterave në një rrjet wireless ad-hoc?
- Cilët janë protokollet dhe strukturat ekzistues të komunikimit internaval në botë?
- Po në Shqipëri, veçanërisht në Vlorë?
- Cilat janë specifikat e dallimit të rrjetit të anijeve nga rrjeti i makinave në rastin e inter-vehicle communications,etj.
- Cilat do të ishin përdorimet e një protokolli të veçantë për komunikimet naval
- A ekziston një përfitim qualitativ në përdorimin e këtij protokolli?
- Si do te përcaktohet vendodhja e çdo anije në çdo cast të kohës?
- Pse zgjedh simulatorin NS2?
- Në cilat kushte supozohet të realizohen simulimet?

Ideja kryesore: në protokollin InterNavComm është krijimi i një infrastrukture virtuale të përbërë nga qeliza me dimensione të caktuara(300-400m) dhe për çdo qelizë zgjidhet një anije që të shërbejë si qendër komunikimi për anijet e tjera në atë zonë. Kjo do të jetë baza e strukturës hierarkike të rrjetit ad-hoc të krijuar për anijet.

Ne i konsiderojmë anijet si nyje të një rrjeti ad-hoc, të ndarë në qeliza virtuale që formojnë infrastrukturën virtuale specifike për këtë protokoll. Nyjet në një sipërfaqe të madhe, që mund të përfaqësojë sipërfaqen e zonës rreth portit, janë organizuar në dy nivele të hierarkisë. Çdo nyje ka pozicionin gjeografik të dhënë nga GPS.

Në nivelin e parë janë përfshirë të gjitha nyjet në një qelizë. Këto nyje komunikojnë me njëra-tjetrën dhe ato gjithashtu mund të komunikojnë me nyjet e qelizave respektive fqinjë, të cilat janë në një fushë ose linjë komunikimi.

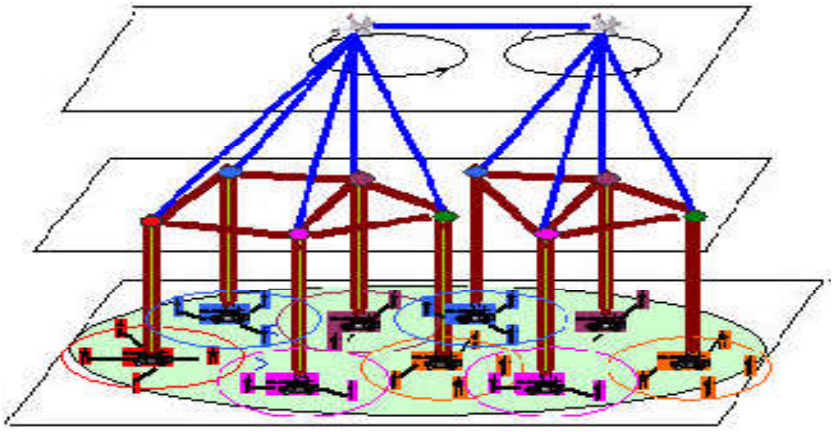


Figura 4.1. Komunikimi hierarkik i nyjeve në një rrjet ad- hoc

Niveli i dyte hierarkik është i përfaqësuar nga ato që i quajme Qendra_Qelizë(Cel_Center-CC), të cilat janë një grup i vogël nyjesh të vendosura afër qendrës gjeografike të çdo qelizë. Qendra_Qelizë mund të komunikojë me antarët e qelizave respektive ose antarët e qelizave fqinjë që janë në një linjë komunikimi me CC. Komunikimi ndërmjet nyjeve të një qelize me atë të CC respektive përfaqëson komunikimin e nivelit te dytë të hierarkisë me nivelin e parë.

Komunikimi ndërmjet anëtarëve në nivel të dytë të hierarkisë përfaqësohet nga komunikimi midis Qendra_Qelizë. Kjo është e mjaftueshme që ato të komunikojnë në mënyrë sekuenciale njëra pas tjetrës kështu që çdo Qendër_Qelizë mund të komunikojë me njërën nga CC fqinjë. Qendrat_Qelizë fqinje sillen si pjesë e zinxhirit që lidh qendrën aktuale(korente) me gjithë gjatësinë e rrugës në tërësi. Ne mendojmë apo supozojmë se CC_at kanë një rang transmetimi të tillë që të mund të mbulojnë prezencën e vrimave që mund të krijohen midis qelizave.

Është e rëndësishme të theksohet se pozicioni i CC optimizon(përmirëson) komunikimin brenda qelizës dhe me qelizat fqinjë, duke mundësuar që të ketë cilësi të ngjashme transmetimi thuajse me të gjithë antarët e qelizës.Përveç kësaj, çdo CC mban pothuajse një cilësi simetrike në komunikimin me qendrat fqinjë(më të afërta), duke siguruar kështu një barazpeshë ose cilësi të ekuilibruar për të dy drejtimet e lëvizjes së informacionit. Pra

kërkesa e vetme për të qenë një CC është që të jetë në një linjë komunikimi me antarët Qelizë. Në këtë filozofi dhe këndvështrim do të vazhdoj të shtrihet studimi im.

Supozohet se një mesazh emergjence duhet të transmetojë ose shpërndahet menjëherë dhe në numër minimal hopesh ky mesazh duhet të merret nga të gjitha nyjet. P.sh në rastin e përmbytjes(flooding) do të kishim një mbingarkim të rrjetit duke rezultuar në humbje të sinjalit dhe vonesa në komunikim. Duke përdorur këtë infrastrukturë virtuale, pra protokollin InterNavComm, ngarkesa e rrjetit bie ndjeshëm, bëhet broadcast vetëm te liderat e qelizës dhe këta të fundit te çdo anije në veçanti.

4.2 Implementimi NS2dhe Vlerësimi i Protokollit InterNavComm me Anë te Simulatorit

4.2.1 Protokolli i Propozuar dhe Transmetimi në Rrjetin e Gjerë.

Në pjesën më të madhe të protokolleve të rutimit të zhvilluara për rrjetet ad-hoc wireless, performanca e transemtimit në rrjet nuk është e kënaqshme edhe për shkak se pjesa më e madhe e këtyre protokolleve bazohen mbi flooding. Duke përdorur këtë teknikë, rrjedhimisht këto protokolle nuk mund të kenë peformancën e duhur në komunikimet pikë me pikë dhe në situatat e emergjencës. Kështu, në mënyrë që të përmirësojmë cilësinë e komunikimeve pikë me pikë, ne propozuam në këtë punim një protokoll të ri, protokollin InterNavComm që ka një strukturë hierarkike.

Ne supozuam se varkat lëvizin në të njëjtin drejtim dhe në të njëjtën hapsirë gjeografike, ku secila varkë njeh pozicionin dhe destinacioni e vet duke përdorur GPS, kanë fuqi optimale për transmetim, dhe ekziston një protokoll i tillë që secila nyje të transmetojë pa interferenca, ky është protokolli MAC(Medium Access Controll). Gjithashtu ne supozuam që kjo hapsirë është ndarë në qeliza virtuale duke patur të njëjtën gjatësi optimale të barabartë, gjatësi që mund të lejojë transmetim dhe marrje optimale të mesazheve. Për të tilla raste një zgjedhje e mirë do të ishte IEEE802.11(kemi folur në kapitujt më sipër) si dhe gjithshtu përzgjedhja e gjatësisë së qelizës të jetë midis 300-400m.

Në figurën 4.2 është ilustruar koncepti i GPS dhe rrjetit sensor ad-hoc wireless për marinën, në një hartë të vendit tonë, Shqipërisë mbi veprimin e varkave të vogla për peshkim si nyje

transmetimi/rele. Si dhe kombinimin e veprimit Ruter +Antenë + GPS, si dhe ndërveprimin me protokollin tonë të rutimit InterNavComm.

Aplikacionet e Monitorim, Kërkim dhe Shpëtimit (MSnR), veprohet si më poshtë: Lidhja përpara nga toka në det (shigjeta e kuqe në Fig. 4.2) përdor sistemin aktual radio me fuqi të lartë stacion - bazë përgjatë vijës bregdetare për të transmetuar motin dhe informacione të rëndësishme për të gjitha anijet e peshkimit.

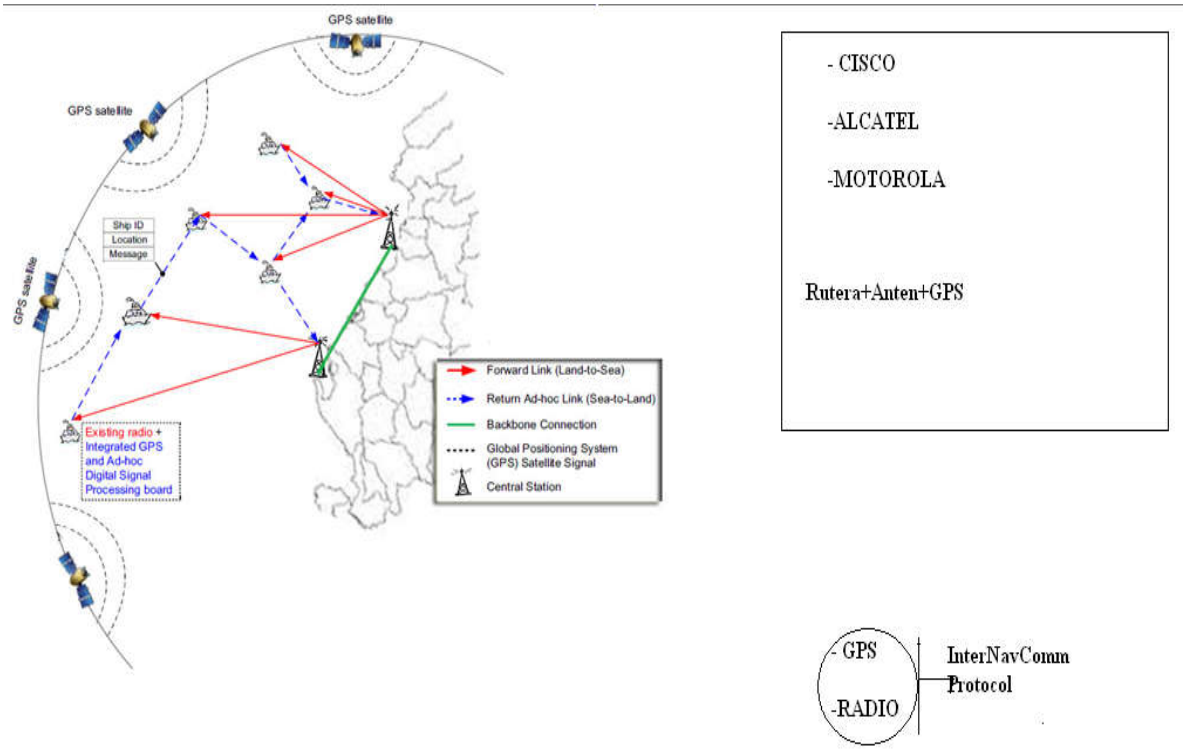


Figura 4.2. Ilustrimi i konceptit GPS dhe rrjetit sensor ad-hoc wireless për marinën, në një hartë të Shqipërisë

Në këtë studim, është spërzgjedhur frekuenca Tx/Rx i 8.294 MHz [44] (sipas spektrit elektromagnetik fig.4.3). Për shkak se antenat transmetuese janë të montuar në stacione-bazë në një lartësi tipike prej 100 metra dhe një fuqi e lartë është në dispozicion, kjo lidhje

[44] ISM/SRD License-Free Frequency Bands

përpara mund të arrijë të gjitha anijet e peshkimit në horizont. Në kontrast me lidhjen përpara, lidhja e kthimit nga deti në tokë (shigjetat blu në Fig.4.2) është i kufizuar nga fuqia e ulët dhe lartësia e antenës e instaluar në të gjitha anije e vogla të peshkimit. Ky problem rregullohet nga ***rrjeti sensor wireless ad hoc***, i cili lejon lidhjen e kthimit që do të krijohet për herë të parë ndërmjet të gjitha anijeve të peshkimit dhe të lidhur nga anijet më të afërt të stacioneve-bazë qëndrore.

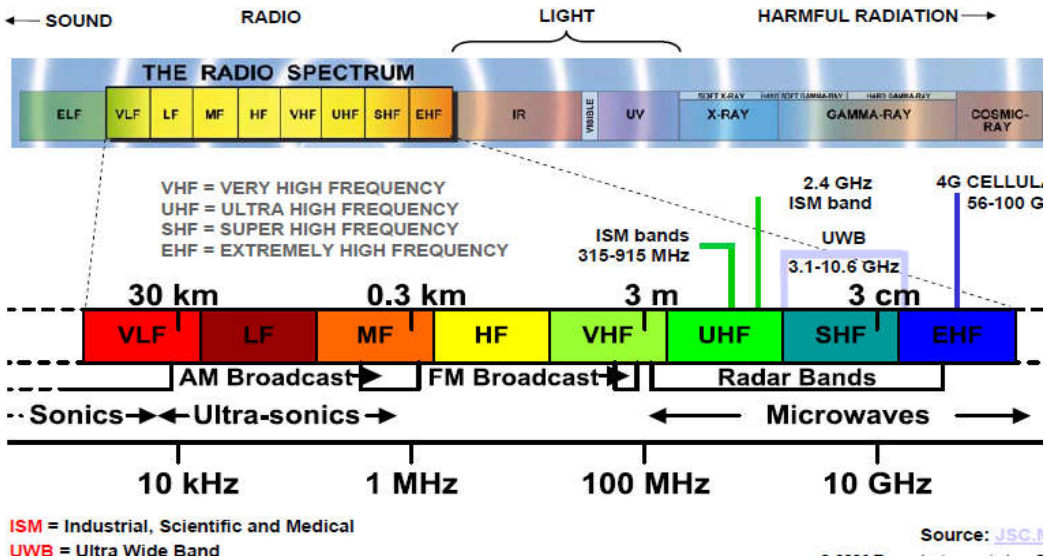


Figura 4.3. Spektri elektromagnetik(Texas instrument Inc, 2006)

Përshkrimi i Përgjithshëm i Strukturës

Ndajmë zonën më të afërt bregdetare në qeliza virtuale që përmbajnë nyje të një rrjeti ad hoc, ku si të tilla merren anijet, varkat etj. Këto qeliza lëvizin së bashku me shumicën e nyjeve të tyre. Prandaj, një infrastrukturë fleksibël virtuale është krijuar dhe mirëmbahet për të mundësuar komunikim të shkallëzuar dhe efektiv. Në çdo qelizë kemi zgjedhur një ose më shumë qendra qelizë (CC-Cell Center).

Në nivelin e parë hierarkik janë përfshirë të gjitha nyjet në një qelizë. Këto nyje komunikojnë me njëra-tjetrën dhe gjithashtu mund të komunikojnë edhe me nyjet respektive fqinje që janë në rangun e komunikimit.

Niveli i dytë i hierarkisë përfaqësohet CC që siç e kam theksuar më lartë janë një grup i vogël nyjesh të vendosura zakonisht afër qendës gjeografike të qelizës. CC mund të komunikojnë me antarët e qelizave fqinje që janë në të njëjtin rang komunikimi të CC. Dhe komunikimi midis nyjeve të një qelize me CC_at respektive përfaqëson komunikimin e nivelit të dytë të hierarkisë me nivelin e parë. Komunikim është në mënyrë sekuenciale kështu që çdo CC mund të komunikojë me CC_at fqinjë. Pozicioni i CC_ve optimizon komunikimin brenda qelizës dhe me qelizat fqinje. Çdo CC mban pothuajse një cilësi/kualitet simetrik në komunikimin me qendrat fqinje, duke siguruar cilësi të balancuar për të dy drejtimet e lëvizjes së informacionit.

Figura 4.4. Struktura hierarkike në proçesin e rutimit. Zona afër portit Vlorë

Struktura hierarkike mundëson optimizimin e procesit të rutimit. Zona e portit është e ndarë në qeliza virtuale, të cilat lëvizin siç lëvizin nyjet, fig.4.4.

Çdo qelizë ka një qendër, e cila është zgjedhur nga anëtarët e qelizave dhe është e vendosur afërsisht në qendër gjeografike të qelizës. Në një normë të caktuar çdo nyjë përditëson të dhënat nga GPS, e cila jep koordinatat (x, y) për çdo nyje në një moment të caktuar.

Anëtarët qelizë zgjedhin një qendër që do të sillet për një interval të caktuar kohor, si një stacion bazë(BS). Çdo nyjë ka pozicionin e saj gjeografik të dhënë nga Global Positioning System (GPS).

Kur një nyje burim ka një mesazh për një nyje destinacion, ia dërgon atë në Cell Center_in e saj. Atëherë mesazhi është përcjellë përmes Qendrave të tjerë Cell. Cell Center së pari verifikon nëse nyja destinacion i përket qelizës së tyre. Së fundi Cell Center destinacion do ta dërgoje mesazhin tek nyja destinacion.

Niveli i tretë përfaqësuar nga NC(Network Centers[45]) të cilat janë një grup i vogël nyjesh të lidhura afër qendrës gjeografike të rrjetit. NC mbajnë të update_uar informacionin e vendodhjes për të gjitha nyjet në rrjet duke siguruar informacionin për CC.

Llogaritja e Kompleksiteti të Komunikimit dhe Kohës për algoritmin tonë të rutimit*:*

Nëse dy nyje në rrjet komunikojnë me njëri-tjetrin, atëherë ne duhet të llogarisim *kompleksitetin e komunikimit* ndërmjet tyre duke përdorur bazën matematikore. Kompleksiteti i Komunikimi është një masë asimptotike e numrit të mesazheve të dërguara në rrjetin gjatë shtrirjes kohore të algoritmit. Për shembull, në qoftë se unë kam një rrjet të plotë (dmth, një grafik të plotë), dhe algoritmi me dërgon të gjithë fqinjët e mi, pastaj algoritmi përfundon mbi secilin procesor, numri i mesazheve të dërguar është n (n-1) i cili është në O (n ^ 2).

Kompleksiteti i kohës së një algoritmi vlerëson sasinë e kohës që një algoritmi i duhet për të vepruar/ekzekutuar në funksion të madhësisë së input_it të problemit. Kompleksiteti i kohës së një algoritmi zakonisht shprehet duke përdorur simbolin O. Ku simboli O është një kufi i sipërm, që shpreh kohën më të keqe të nevojshme në të cilin vepron një algoritëm për inputet e ndryshme. Megjithëse, disa inpute mund ta lejojnë algoritmin të veprojë/ekzekutojë më shpejt.

Transmetimi i rrjetit të gjerë është një tipar thelbësor për rrjetet pa tel. Metoda më e thjeshtë për shërbimin e transmetimit është përmbytja/flooding. Ndër përparësitë e saj është

[45] Qendrat e rrjetit

thjeshtësia, megjithatë, për një transmetim të vetëm, përmbytja gjeneron ritransmetime të bollshme që ndikojnë në fuqinë e baterisë dhe humbje të bandwidth. Gjithashtu, ritransmetimet e nyjeve të afërta kanë gjasë të ndodhin në të njëjtën kohë. Si rezultat, flooding shpejt çon në përplasje mesazh dhe zënie kanali. Ky është i njohur si problemi stuhi transmetimi. Për shkak të disa karakteristikave qenësore të përbashkëta ndërmjet rrjeteve sensor dhe rrjeteve Mobile ad hoc (MANETs) të gjithë protokollet e transmetimit të propozuara për MANETs mund të zgjerohen për rrjetet sensor. Problemi i transmetimit është studiuar gjerësisht për rrjetet multihop. Zgjidhjet optimale për të llogaritur Minimum Connection Domination Set (MCDS) janë marrë për rastin kur çdo nyje e di topologjinë e të gjithë rrjetit (transmetimit centralizuar). Protokolli i transmetimit përfundon transmetimin e një mesazhi në O (Dlog2n) hapa, ku 'D' është diametri i rrjetit dhe 'n' është numri i nyjeve në rrjet. Nga rezultatet, ky protokoll është optimal për rrjetet me diametër konstant. Për rrjetet me një diametër më të madh, një protokoll nga Gaber et al e përfundon transmetimin brenda O (D +) log5n time slots[46], dhe kjo është optimale për rrjetet me D ∈ (log5n). Këto zgjidhje janë përcaktuese dhe garantojnë një vonesë kufizuese në shpërndarjen e mesazhit, por kërkesa që secila nyje duhet të dijë të gjithë topologjinë e rrjeti është një kusht i fortë, jopraktik për tu mbajtur në rrjetet wireless.

Përsa i përket algoritmit tonë të rutimit, proçedura e përcjelljes së mesazhit nga një burim S në një destinacion D jepet në mënyrë skematike në figurën 4.5, ku CC përcaktohen si BS(Stacione Bazë) sepse ato luajnë rolin e stacioneve bazë virtuale.

[46] Time slot është një koncept në rrjetet kompjuterike. Ky është të paktën dyfishi i kohës që duhet për një impuls elektronik (OSI Shtresa 1 - Fizike) për të 'udhëtuar' në gjatësinë e distancës maksimale teorike midis dy nyjeve

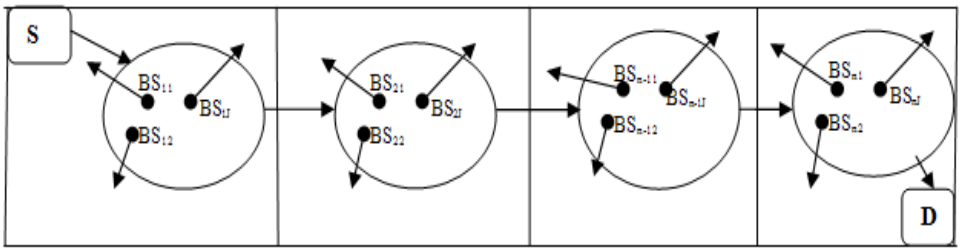


Figura 4.5. Skematizimi i përcjelljes së mesazhit duke përdorur qendrat virtuale.

Në situata të veçanta ku burimi S 'është i vendosur në rangun e komunikimit të CCi + 1 dhe kjo është edhe më afër destinacionit sesa CCi, mesazhi do të përcillet direkt me CCi +1.

Një situatë e ngjashme ndodh kur destinacion D është në rangun e komunikimit te BS të mëparshëm. Mesazhi është përcjellë drejtpërdrejt nga CCd-1 tek D (CCd është CC për destinacionin D). Numri maksimal i hop_eve në nyjen destinacion është **(L + 2),** ku L është numri i hop_eve ndërmjet CCs. Për një rrugë të drejtë, L zakonisht paraqet diferencën në treguesit CCs . Skematikat përjellëse tek figura 4.5. përdorin CCs virtuale. Tabela kurs hyrëse janë krijuar gjatë shkëmbimit të parë të mesazhit "hello" dhe janë përditësuar më pas në çdo interval update_uar. Madhësia e tabelës së rutimit është minimale dhe është i harmonishëm/ akordueshëm në kuptimin që për trafik të lartë dhe densitet të nyjeve të lartë një gjatësi qelizë më e vogël përdoret. Nëse numri i nyjeve në një qelizë është n, rendi në tabelën e rutimit është O (n). Kur tabela e kursit zgjerohet për të përfshirë hyrjet për të gjitha nyjet në rangun e komunikimit, rendi është O (2 n), (duke pasur parasysh një shpërndarje afërsisht uniforme të nyjeve).

4.2.2 Hapat për ndërtimin e Algoritmit.

Protokolli i propozuar: InterNavComm, komponentet e protokollit tonë:

- ***Krijimi Struktures***. Algoritmi fillon me krijimin e infrastrukturës virtuale. Nyjet e së njëjtës qelizë ose e qelizave fqinje, që janë brenda rrezes së komunikimit shkëmbejnë mesazhin fillestar "Përshëndetje". Si rezultat çdo nyjë e di pozicionin e të gjitha nyjeve që mund të komunikojnë me të. Në mënyrë që të kemi të dhënat e fundit, pozita e çdo nyje është përditësuar periodikisht duke shkëmbyer mesazhe "Hello". Në protokollin

tonë procesi i update është njësoj si i rutimit gjeografik ndërkohë që nyjet lëvizin në të njëjtin drejtim dhe afërsisht me të njëjtën shpejtësi mesatare në vijë të drejtë. Intervali i update_imit varet nga lëvizshmëria e nyjes, nëse kjo lëvizshmëri është e lartë nevojitet një interval i shkurtër update.

Të gjitha nyjet vendosin/ krijojnë antarët qelizë duke patur parasysh që të kenë një distancë të shumëfishuar me 400m. Shënojmë me X_0 dhe Y_0 koordinatat e kufirit të qelizës së parë. Në çdo qelizë secila nyje shkëmbenë mesazhin *Hello* duke përfshirë: koordinatat e nyjes së parë, pozicionin korent të nyjes, shpejtësinë aktuale, numrin aktual të qelizave.

Numri aktual i qelizave llogaritet si:

$$Numer\_Qelizave = \left\lfloor \frac{D}{400} \right\rfloor$$

$$D = mod400\sqrt{(my\_X - X_0)^2 + (my\_Y - Y_0)^2}$$

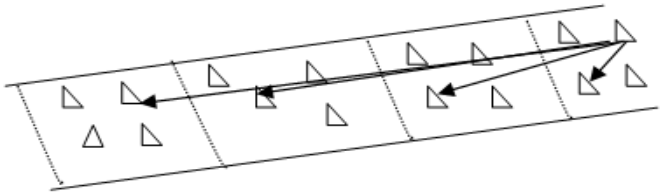
ku D-distanca euklidiane midis nyjes me koordinata $(my\_X; my\_Y)$ dhe kufirit të qelizës së parë. Për një performancë më të mirë, mesazhet *Hello* shkëmbehen midis nyjeve të afërta që i pëkasin nyjeve fqinje.(M.Durresi, 2005 IEEE)

- ***Përzgjedhja e Qendrës_Qelizë***. Anëtarë të së njëjtës qendër_qelizë marrin pjesë në procesin e përzgjedhjes së Cell Center_ve përkatëse. Qendra Cell janë vetë zgjedhur si nyje duke qenë në një gamë të caktuar minimale në afërsi të qendrës së qelizës dhe duke pasur cilësi të mirë të pritjes sinjal.

  - Procesi i numërimit të qelizave: Gjatë këtij proçesi së pari çdo anije merr nga GPS informacionin mbi pozicionin e koordinatave x dhe y. Anija e parë që nuk arrin qelizat e tjera konsiderohet si qeliza pikënisëse ose me kufi 0 që transmeton, me koordinata (X_0, Y_0). Kjo qelizë ia transmeton pozicionin dhe informacionin e vet të gjitha nyjeve që janë brenda rangut të komunikimit. Të gjitha nyjet brenda këtij rangu komunikimi vendosin/krijojnë automatikisht antarët qelizë respektiv dhe i deklarojnë ato tek të gjitha nyjet në qelizë duke shkëmbyer mesazhet “Hello“ duke

përfshirë: ID e nyjes; koordinatat X_0, Y_0; pozicionin e nyjes korente; shpejtësia korente dhe numri aktual i qelizave. (M.Durresi, 2005 IEEE)

Procesi i numërimit të qelizave ilustrohet me anë të figurës më poshtë:



Figurë 4.6. Proçesi i numërimit të qelizave në vijë të drejtë

- ***Komunikimi Pikë-me-pikë*** **.** Ky algoritmi përcakton veprimin e nyjeve dhe CC_at për komunikimet burim-destinacion. (M.Durresi, 2005 IEEE)

1. nyjet burim përfshihen në qelizën *i*:
   - kontrollo drejtimin e komunikimit me destinacionin nëse distanca është:

$$d = \sqrt{(X_d - X_s)^2 + (Y_d - Y_s)^2}$$

2. përndryshe përcill mesazhin tek qendër_qeliza e vet ose në stacionin baze(BS) të tij, pasi vet CC mund ti konsiderojme si BS. Pas marrjes së mesazhit BS e dërgon atë tek BS($X_{\_bs}$,$Y_{\_bs}$) që është afër destinacionit. Stacioni bazë më i afërt do të ketë distancën minimale për në destinacion (*d_BS_min*) të llogaritur më poshtë:

$$d\_BS\_min = min\sqrt{(X_{bs} - X_d)^2 + (Y_{bs} - Y_d)^2}$$

3. Pas marrjes së një mesazhi të ri një qendër BS, së pari kontrollon në tabelën e tij të rutimit nëse destinacioni është një antarë e kësaj qelize. Nëse jo ai vazhdon proçesin përpara tek qendrat e tjera duke aplikuar të njëjtin algoritëm në mënyrë që mesazhi të shkojë përpara në destinacion. Nyja burim menjëherë transmeton mesazhin tek të gjitha nyjet në qelizën ku bën pjesë. Më pas qeliza BS_{ij}, ku bën pjesë kjo nyje, e dërgon mesazhin, duke u bazuar në politikat e veta, tek qendrat e tjera fqinje. Çdo qendër tjetër e transmeton këtë mesazh duke ndjekur një politikë skedulimi si në figurën 4.6. Në një numër minimal hope_sh destinacioni

merr mesazhin. Transmetim i komunikimit mund të bëhet i nevojshëm sidomos në rastet e emergjencës.

- ***Transmetim i Komunikimit***. Algoritmi përcakton veprimin për nje komunikim te pjesshëm ose të plotë të transmetuar në rrjet. Struktura hierarkike e protokollit është veçanërisht e përshtatshme për komunikimet elektronike.

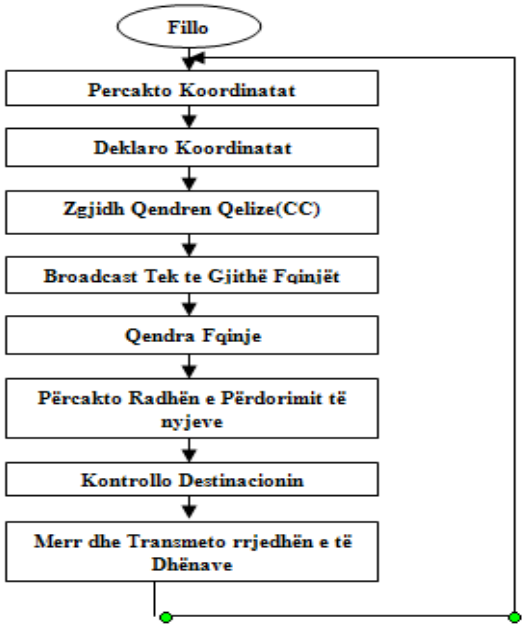


Figura 4.7. Bllok-skemë e thjeshtë për marrjen dhe transmetimin e të dhënave në rrjet

4.2.3 Vlerësimi I performancës së protokollit InterNavComm. Kodi dhe Rezultati nga Simulimet me Simulatorin NS2

Për të vlerësuar performancën e protokollit marrim parasysh 2 metrika:

Vonesa (End-to-End) Pikë me pikë, e matur ne ms. Kjo përdoret për shkëmbim informacionit ndërmjet burimeve dhe destinacioneve të ndryshme të marra rastësisht dhe që kanë distancë të ndryshme ndërmjet tyre. Sigurisht rezultatet varen nga ngarkesa e trafikut, shpeshtësia e mjeteve, ne kemi përdorur metrikun për distancë të normalizuar, figura

4.8.(kodi për end-to-end delay, është shfaqur dhe sqaruar tek pjesa e gjithë kodit të protokollit, si më poshtë)

Distance	RTT ms
100	2
200	2
300	2
400	2
500	3
600	3
700	3
800	4
900	4
1000	4
1100	5
1200	5
1300	6
1400	7
1500	8

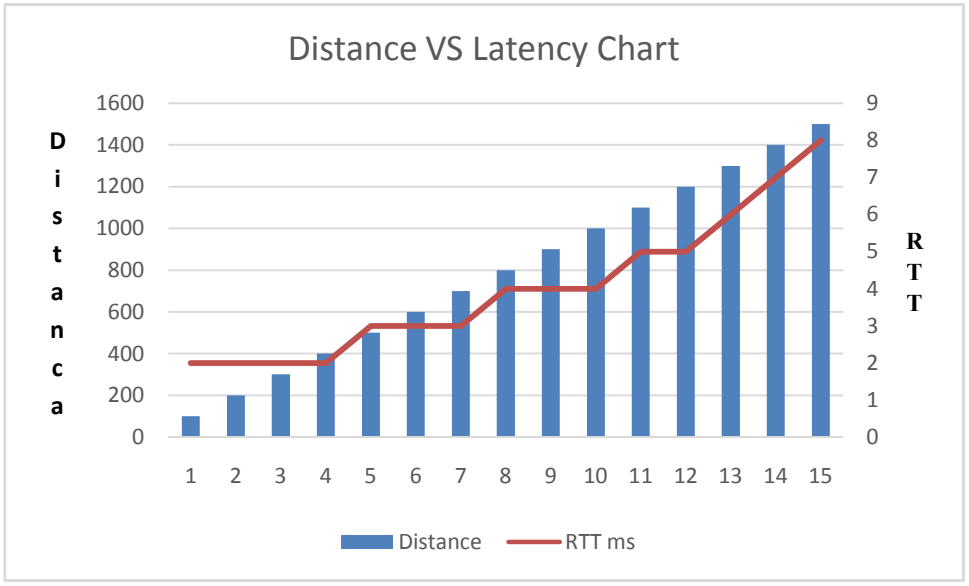


Figura 4.8. Ku paraqitet vonesa pikë me pikë(end- to-end delay), shoqëruar me të dhënat në tabelë.

End-to-fund vonesa i referohet kohës që duhet marrë për një paket që do të transmetohet nëpër një rrjet nga burimi në destinacion. Ky është një term i zakonshëm në IP, dhe ndryshon nga koha vajtje-ardhjet, RTT(Round Trip Time).

Vonesa fund-me-fund është llogaritur ndërmjet dy pikave të sinkronizuara A dhe B të një rrjet IP, dhe se paraqet kohën që një paket kalon gjatë një udhëtimi përmes gjithë rrjetit IP nga A në B.

Paketat e transmetuara duhet të identifikohen në burim dhe destinacion në mënyrë për të shmangur humbjen e paketës apo riorganizimin e saj. Metoda e matjes bën të qartë se kjo vlerë është në thelb e ndryshme nga RTT/ 2 value.

dend-end= N[dtrans+dprop+dproc+dqueue]

ku:

$d_{end-end}$= end-to-end delay(vonesa fund me fund)

d_{trans}= transmission delay(vonesa e transmetimit)

d_{prop}= propagation delay(vonesa e përhapjes)

d_{proc}= processing delay(vonesa e proçesimit)

d_{queue}=Queuing delay(vonesa e radhitjes)

N= number of links (Number of routers - 1)(nr. i linke_ve)

Each router will have its own d_{trans}, d_{prop}, d_{proc} hence this formula gives a rough estimate.

Këto katër komponentë ndahen më tej:

1. Përpunimi nyje:
    - Kontrolloni gabimet të bit_it
    - Përcaktoni link_un e daljes
2. Radhitja:
    1. Koha duke pritur linkun e daljes për transmetim
    2. Varet nga niveli i ngjeshjes(kongjestionit) të ruterit
3. Vonesa e Transmetimit:
    1. R=Link bandwidth (bit/s)
    2. L=Packet length (bits)
    3. Time to send bits into link = L/R
4. Vonesa e Përhapjes:
    1. d = Length of physical link
    2. s = Propagation speed in medium

3. Propagation delay = d/s

Duke u nisur edhe nga të dhënat e paraqitura në tabelë dhe kurba e grafikut siç tregohet në figurën 4.9 ne krahasojmë end-to-end delay midis protokollit InterNavComm dhe Flooding(i jemi referuar grafikut të nxjerrë nga paper i M.Durresi, A.Durresi, L.Barolli, 2007 IEEE) për komunikime të ndryshme ndërmjet nyjeve me një distancë të dhënë siç është treguar në grafikun më lartë. Për nyje të afërta të dy së bashku protokolli InterNavComm dhe Flooding performojnë thuajse njësojë. Por vërejmë qartë se protokolli ynë InterNavComm është një protokoll i shkallëzueshëm(scalable), që performon shumë më mirë për nyje më në distancë, dhe me një vonesë pikë me pikë(end-to-end delay) më të vogël se Flooding. Kjo shpjegohet edhe me faktin se, në krahasim me flooding duke përdorur një skemë hierarkike edhe numri i mesazheve që do të shkëmbehet do të jetë i njëjtë me qelizat ndërmjet burimit dhe destinacionit plus 2(pra një komunikim midis nyjes burim dhe CC_it të tij më të afërt dhe CC_it të fundit tek destinacioni). Numri i mesazheve të shkëmbyera nga Flooding është më i lartë dhe numri i mesazheve të shkëmbyera rritet shumë shpejt me rritjen e nr. të nyjeve gjatë komunikimit. Në protokollin tonë të rutimit ky numër është më i vogël.

Ngarkim rutimi, i matur në bazë të numrit të mesazheve që transmetohen për çdo burim komunikimi në destinacion. Për të patur ide më të qarta, protokollin tonë të rutimit e krahasojmë me protokolle të tjera rutimi, p.sh me një protokoll të njohur të përdorur në rastin kur kemi vërshime ose e njohur ndryshe “përmbytje”.

Për të dy protokollet, krahasohet numri total i mesazheve të shkëmbyera ose ngarkim rutimi për çdo burim-destinacion dhe nxjerrim si përfundim se cili prej protokolleve, protokolli i paraqitur prej nesh paraqet performancën më të lartë.

Shumë protokolle rutimi të zhvilluar për rrjetet ad-hoc wireless janë modifikuar dhe adaptuar për përdorim në sistemet e transportit. Në pjesën më të madhe të këtyre protokolleve performanca nuk është e kënaqshme për shkak të rrugës proçesi i zbulimit i bazuar në përmbytjen(flooding) dhe si rrjedhojë këto lloj protokolle nuk mund të kenë

performancën e duhur për komunikimet pikë me pikë dhe në situatat e emergjencës. Për t'i ardhur në ndihmë kësaj situate ne propozojmë protokollin tonë të rutimit InterNavComm.

InterNavCom është një algoritëm jo-uniforme table-driven, me ndarje faktike të zonës dhe bazuar në kurs gjeografike. Ky protokoll bën më eficient përdorimin e burimeve dhe shmang proçesin e zbulimit të kursit (protokollet reaktive).

Supozime dhe modeli i Simulimit

Ne zbatojmë një skemë rutimi multihop ku simulatori i përdorur është NS2. Në këtë eksperiment apo simulimet tona supozojmë se rrjeti përbëhet nga afërsisht 50 nyje roaming në një hapësirë 1000x1000 metër. Zona roaming për rrjetin me madhësi 50, 200, 400 dhe 1000 është respektivisht 700x700, 1500x1500, 2000x2000 3000x3000 metër katror. Gama e transmetimit radio është 120 metra dhe kapaciteti i kanalit është 2Mbits/sec. Ne përdorim protokollin MAC IEEE 802.11 me Funksioni Shpërndarje Koordinimi (DCF) si shtresa MAC në eksperimentet tona.

Packet Delivery Ratio[47](PDR)

Packet Delivery Ratio është raporti i paketave të të dhënave të ofruara/shpërndara për destinacionet kundrejt paketave të të dhënave të rifituara/marra nga burimet. Ky numër paraqet efektivitetin e protokollit të rutimit.

- **Kodi për Simulimin e lëvizshmërisë së varkave.**

SIMULIMI i Protokollit ad-hoc tek Varkat në levizje:

 # Si fillim do të bëhet deklarimi i pjesëve përbërëse të tilla si: Lloji i kanalit te komunikimit; Lloji i ndërfaqeve të rrjetit; Shtresa e linkut, link layer type.....

```
set val(chan)        Channel/WirelessChannel        ;# Lloji i kanalit te komunikimit
set val(prop)        Propagation/TwoRayGround       ;# Modeli i radio-propagation
set val(netif)       Phy/WirelessPhy                ;# Lloji i nderfaqeve te rrjetit
```

[47] Raporti I dorëzimit të paketave

```
set val(mac)          Mac/802_11                    ;# Lloji i MAC (media access control)
set val(ifq)          Queue/DropTail/PriQueue       ;# interface queue type
set val(ll)           LL                            ;# Shtresa e linkut, link layer type
set val(ant)          Antenna/OmniAntenna           ;# Modeli i antenave
set val(ifqlen)       50              ;# Numri max i paketave ne ifq (interface priority queue)
set val(nn)           10              ;# numri i varkave ne levizje
set val(rp)           InterNavComm      ;# protokolli i rutimit
set val(x)            500             ;# Kordinatat/Dimesnionet ne rrafshin horizontal X
set val(y)            400             ;# Kordinatat/Dimesnionet ne rrafshin vertikal Y
set val(stop)         150             ;# Koha kur simulimi mbaron
set ns        [new Simulator]
set tracefd     [open test InterNavComm.tr w]
set windowVsTime2 [open win.tr w]
set namtrace    [open test InterNavComm.nam w]
$ns trace-all $tracefd
$ns namtrace-all-wireless $namtrace $val(x) $val(y)
# konfigurimi i vendodhjes se varkes
set topo      [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
#
```

Pasi bëhet deklarimi i pjesëve përbërse, në vazhdim do të ndërtojmë kodin për krijimin e nn VARKA [$val(nn)] dhe më pas do ti lidhim ato në komunikim.

#

 # Konfigurimi i varkave

```
        $ns node-config -adhocRouting $val(rp) \
             -llType $val(ll) \
             -macType $val(mac) \
             -ifqType $val(ifq) \
             -ifqLen $val(ifqlen) \
             -antType $val(ant) \
             -propType $val(prop) \
             -phyType $val(netif) \
             -channelType $val(chan) \
             -topoInstance $topo \
             -agentTrace ON \
             -routerTrace ON \
             -macTrace OFF \
             -movementTrace ON
    for {set i 0} {$i < $val(nn) } { incr i } {
        set node_($i) [$ns node]
        $node_($i) set X_ [ expr 10+round(rand()*480) ]
        $node_($i) set Y_ [ expr 10+round(rand()*380) ]
        $node_($i) set Z_ 0.0
    }
    for {set i 0} {$i < $val(nn) } { incr i } {
        $ns at [ expr 15+round(rand()*60) ] "$node_($i) setdest [ expr 10+round(rand()*480) ]
[ expr 10+round(rand()*380) ] [ expr 2+round(rand()*15) ]"
```

}

 # Gjenerimi i lëvizjeve. Ku do të përcaktohen të gjitha lëvizjet ne rrjet me klasat IP dhe subnetet përkatëse

$ns at 10.0 "$node_(0) setdest 250.0 250.0 3.0"

$ns at 15.0 "$node_(1) setdest 45.0 285.0 5.0"

$ns at 70.0 "$node_(2) setdest 480.0 300.0 5.0"

$ns at 20.0 "$node_(3) setdest 200.0 200.0 5.0"

$ns at 25.0 "$node_(4) setdest 50.0 50.0 10.0"

$ns at 60.0 "$node_(5) setdest 150.0 70.0 2.0"

$ns at 90.0 "$node_(6) setdest 380.0 150.0 8.0"

$ns at 42.0 "$node_(7) setdest 200.0 100.0 15.0"

$ns at 55.0 "$node_(8) setdest 50.0 275.0 5.0"

$ns at 19.0 "$node_(9) setdest 250.0 250.0 7.0"

$ns at 90.0 "$node_(10) setdest 150.0 150.0 20.0"

 # Pikërisht në këtë pikë/pjesë të kodit simulohet ngritja e një lidhje TCP mes varkave 2 dhe 8 , me nje protokoll FTP

set tcp [new Agent/TCP/Newreno]

$tcp set class_ 2

set sink [new Agent/TCPSink]

$ns attach-agent $node_(2) $tcp

$ns attach-agent $node_(8) $sink

$ns connect $tcp $sink

```
set ftp [new Application/FTP]

$ftp attach-agent $tcp

$ns at 10.0 "$ftp start"

set tcp [new Agent/TCP/Newreno]

$tcp set class_ 2

set sink [new Agent/TCPSink]

$ns attach-agent $node_(5) $tcp

$ns attach-agent $node_(0) $sink

$ns connect $tcp $sink

set ftp [new Application/FTP]

$ftp attach-agent $tcp

$ns at 10.0 "$ftp start"
```

Shaqja e dritares se punës

```
proc plotWindow {tcpSource file} {

global ns

set time 0.01

set now [$ns now]

set cwnd [$tcpSource set cwnd_]

puts $file "$now $cwnd"

$ns at [expr $now+$time] "plotWindow $tcpSource $file" }

$ns at 10.1 "plotWindow $tcp $windowVsTime2"
```

 # Është i rëndësishëm deklarimi i pozicioneve të varkës siç është edhe pozicioni filestar, kështu në këtë pjesë do të bëhet deklarimi i pozicionit fillestar të varkës

```
for {set i 0} {$i < $val(nn)} { incr i } {
# 30 percakton madhesine e varkes per nam (network address module)
$ns initial_node_pos $node_($i) 30
}
```

 # Deklarimi i përfundimit të simulimit të varkes

```
for {set i 0} {$i < $val(nn) } { incr i } {
   $ns at $val(stop) "$node_($i) reset";
}
```

 # Dhe si përfundim kjo pjesë e kodit ka të bëjë me mbylljen e simulimit dhe perfundimin e këtij momenti komunikimi mes varkave.

```
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "stop"
$ns at 150 "puts \"end simulation\" ; $ns halt"
proc stop {} {
   global ns tracefd namtrace
   $ns flush-trace
   close $tracefd
   close $namtrace
}
$ns run
```

- **Le të trajtojmë me radhë, duke i shpjeguar, të gjitha ato pjesë kodi që inicializojnë matjen e vonesës pikë me pikë (end to end delay)**

Bit rate, ku do të vendoset edhe koha korente, numri i nyjeve dhe paketave, koha e startimit.

```
cout<<CURRENT_TIME<<endl;
set tcp_(0) [new Agent/TCP]
$ns_ attach-agent $node_(v4) $tcp_(0)
set null_(0) [new Agent/Null]
$ns_ attach-agent $node_(v5) $null_(0)
set cbr_(0) [new Application/Traffic/CBR]
$cbr_(0) set maxpkts_ 1000
$cbr_(0) attach-agent $tcp_(0)
$cbr_(0) set packetSize_ 3
$cbr_(0) set interval_ 0.3
$cbr_(0) set random_ 1
$ns_ connect $tcp_(0) $null_(0)
$ns_ at CURRENT_TIME "$cbr_(0) start"
```

Në këtë pjesë të kodit do të kryhet ngarkimi i rrjetit, burim i rrjetit, vendoset lidhja TCP midis nyjes 4 dhe 5, agjenti është në gjendje të dedektojë një anije të re(nyje te re) vendoset rangu, numri i paketave dhe kryehet aplikimi i ri, ftp.

```
# networkLoad.tcl
set ns $ns_
$ns_ color 1 Green
$ns_ color 1 Red
source trafiku.tcl
# establish TCP connection on node_(4) and node_(5)
set tcp [new Agent/TCP/NewShip]
```

```
$tcp set rate_ 120k

$tcp set packetSize_ 100

set ftp [new Application/FTP]

$ftp attach -agent $tcp

$ns_ at 2.0 "$ftp start"

set sink [new Agent/TCPSink]

$ns_ attach-agent $node_(0) $tcp

$ns_ attach-agent $node_(9) $sink

$ns_ connect $tcp $sink
```

Ndërsa në pjesën e kodit që vjen më poshtë do ti referohemi topologjisë së lëvizjes, ku si fillim përcaktohet origjina për anijet që ndodhen afër ose përgjatë bregut të detit, me tri koordinatat përkatëse x, y, z. Pra vendoset pika e startimit dhe finale për lëvizjen e anijeve/varkave, dhe gjithshtu edhe shpejtësia(fillon me 30 m/s) e tyre.

```
# move.tcl

# set TOPOlogy_Y $val(y)

# The starting origin for the ships along the sea

set ori_x 20.0

set ori_y [expr {$val(y)/30.0}]

set ori_z 0.0

# the final point that the ships move

set final_x 995.0

set final_y [expr {$val(y)/30.0}]

# the speed of the ships along the sea in m/s

set speed 30
```

```
set lane 0
set lanecnt 0
set xpos 0
for {set i 0} {$i < $num_ships} {incr i} {
if {[expr {$i % 10}] == 0} {
incr lane
set xpos 0
}
$node_($i) set X_ [expr {$ori_x + 100 + $xpos * $spacing}]
$node_($i) set Y_ [expr {$ori_y
-
$lane * 15}]
$node_($i) set Z_ $ori_zincr xpos
}
$node_(0) set X_ 5
$node_(0) set Y_ [expr {$ori_y + 30}]
for {set i 0} {$i < $num_ships} {incr i}
{
$ns_ at 0.0 "$node_($i) setdest $final_x $final_y $speed"
}
```

Më në fund kemi arritur tek ajo pjesë e kodit ku do llogaritet End –to end delay i protokollit tonë. Pra skripti i mëposhtëm gjeneron nyjen nga do të fillojë lëvizja si dhe vonesën në trafik pikë me pikë. Vendos kohën për të filluar procedura dhe mbledh kohët, gjerësia e bandwidth_it ruhet në një file dhe rivendos numëruesin

```
# This script generate node movement and traffic delay between end to end devices.
set val (loss)   SignalLoss                    ;# Loss of signal due to weather conditions
set val(chan)    Channel/WirelessChannel       ;# Comunication channel
set val(prop)    Propagation/ThreeRayGround    ;# radio propagation way
set val(netif)   Phy/WirelessPhy               ;# network interface type
set val(ifq)     Queue/DropTail/PriQueue       ;# interface queue type
set val(ll)      LL                            ;# link layer type
set val(ant)     Antenna/OmniAntenna           ;# antenna model
set val(ifqlen)  100                           ;# packet size
set val(nm)      10                            ;# number of ships
set val(rp)      InterNavComm                  ;# routing protocol
set val(x)       1000                          ;# X dimension
set val(y)       20                            ;# Y dimension
set val(stop)    20                            ;# simulation periode
set ns_          [new Simulator]
set node_size 20
set spacing 100
set num_ships $val(nm)
# Record creates periodically records the bandwidth received by
# traffic sinc 0 and writes it to the three files f0
proc record {}
{
global sink f0
```

```
set ns_ [Simulator instance]
# Set the next time to call the prcedure and collect the time and bw
set time 0.5
set bw0 [$sink set bytes_]
set now [$ns_ now]
# Save the bandwidth to a file and reset the counter and set up the next
# time to call record again
puts $f0 "$now [expr $bw0/$time*8/1000000]"
$sink set bytes_ 0
$ns_ at [expr $now+$time] "record"
}
# Printing the window size
proc plotWindow {tcpSource file}
{
global ns_
set time 0.01
set now [$ns_ now]
set cwnd [$tcpSource set cwnd_]
puts $file "$now $cwnd"
$ns_ at [expr $now+$time] "plotWindow $tcpSource $file"
}
proc stop {}
{
```

```
global ns_ tracefd namtrace f0

$ns_ flush-trace

close $tracefd

close $namtrace

close $f0

exec xgraph fourwaytraffic.tr - geometry 800x400 &

#Execute nam on the trace file

exec nam simwrls.nam &

exit 0

}

$ns_trace-all $tracefd

$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)
```

Në këtë pjesë të kodit si fillim konfigurohet protokolli MAC, përdorë standartin 802.11p, krijimi dhe konfigurimi i të githa nyjeve deri në nn numër nyjesh. Përcaktohet modeli i trafikut, pozicioni fillestar i nyjes dhe i tregohet asaj se kur simulimi mbaron, procedura mbaron pas 5 s të kohës së simulimit.

```
# Configure the MAC Protocol to use the 802.11p

standard source IEEE802-11p.tcl

# Initialize the Topography, god object and area

set topo       [new Topography]

set god_ [create-god$val(nm)]

$topo load_flatgrid $val(x) $val(y)

#  Create and configure all the nodes upto nn number of nodes

$ns_ node-config-adhocRouting $val(rp)\
```

```
-lossType $val(lo)\
-llType $val(ll)\
-ifqType $val(ifq)\
-ifqLen $val(ifqlen)\
-antType $val(ant)\
-propType $val(prop)\
-phyType $val(netif)\
-channelType $val(chan)\
-topoInstance $topo\
-movementTrace ON

# set num_nodes [expr {$val(nm) * 2}]
for {set i 0} {$i < $val(nm) } { incr i }
{
set node_($i) [$ns_ node]
}
# Define traffic model
puts "Loading move.tcl file..."
source $val(sc)
puts "Loading networkTraffic.tcl file..."
source $val(cbr)
#Start logging the received bandwidth
$ns_ at 0.0 "record"
```

```
$ns_ at 10.1 "plotWindow $tcp $windowVsTime2"
# Define node initial position in nam
for {set i 0} {$i < $val(nm)} { incr i }
{
# 30 defines the node size for nam
$ns_ initial_node_pos $node_($i) 20
}
# Telling nodes when the simulation ends
for {set i 0} {$i < $val(nm) } { incr i }
{
$ns_ at $val(stop) "$node_($i) reset";
}
# ending nam and the simulation
$ns_ at $val(stop) "$ns_ remote-ship $val(stop)"
$ns_ at $val(stop) "stop"
$ns_ at $val(stop) "puts\"end simulation\" ; $ns_ halt"
#Call the finish procedure after 5 seconds of simulation time
$ns_ run
```

Mbi simulatorin NS2

Ns është një simulator diskret ngjarjesh që drejtohet/tragetohet në hulumtim të rrjeteve. Ns siguron mbështetje të konsiderueshme për simulimin e TCP, rutimit, dhe protokolleve multicast mbi rrjetet me tel dhe pa tel (lokale dhe satelitore). Ns filloi si një variant i simulatorit të rrjetit REAL në vitin 1989 dhe ka evoluar ndjeshëm gjatë viteve të fundit. Në

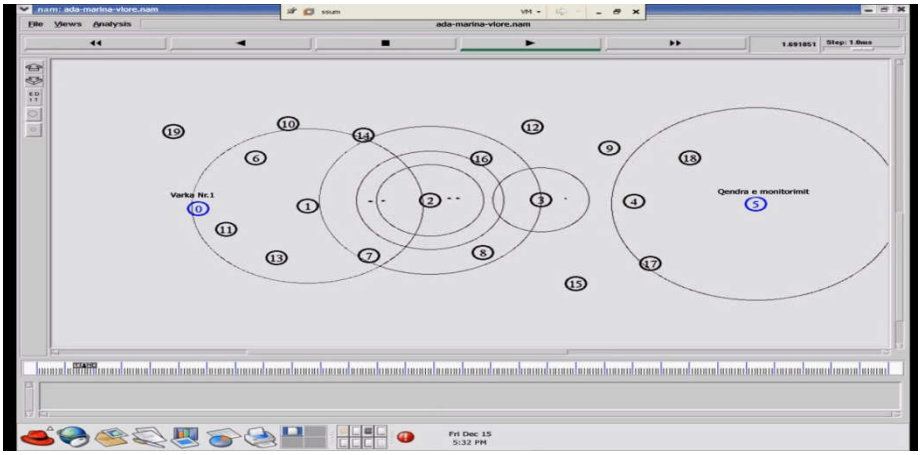
1995 zhvillimi ns u mbështet nga DARPA përmes projektit VINTnë LBL, Xerox Parc, UCB dhe USC / ISI. Aktualisht zhvillimi i ns mbështetet përmes DARPA me SAMAN dhe përmes NSF me CONSER, në bashkëpunim me studiues të tjerë, duke përfshirë ACIRI. Ns ka përfshirë gjithmonë kontribute të ndjeshme nga studiues të tjerë, duke përfshirë kodin wireless nga projektet UCB Daedelus dhe CMU Monarku dhe Sun Microsystems. NS-2 punon në nivel pakete dhe është kryesisht i bazuar te Unix. Përdor TCL si gjuhë kriptimi.

Parametrat e Simulimit

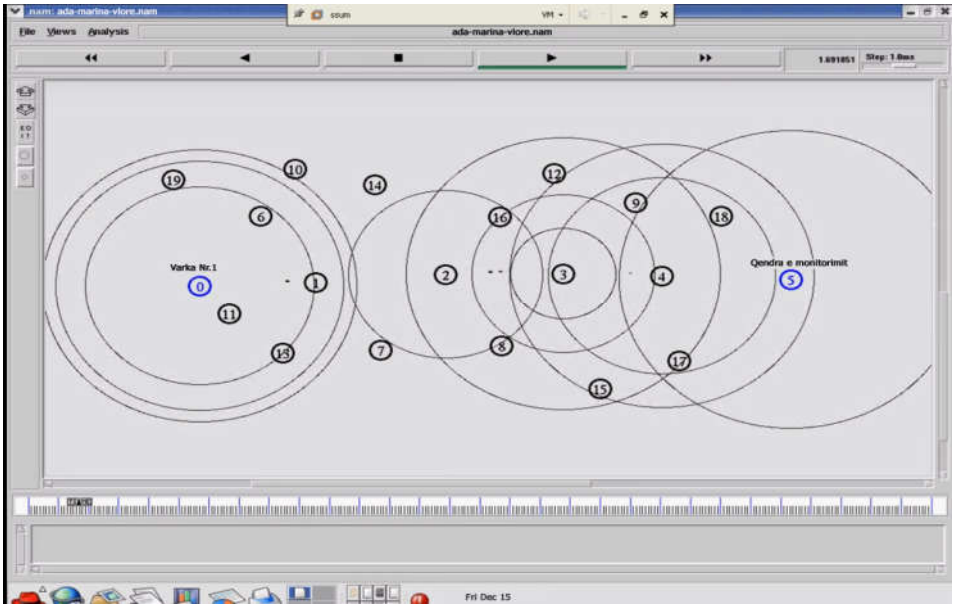
Numri i Nyjeve(vehicles)	10-50
Hapësira e simulimit	1000m*1000m
Gjerësia e qelizës	300m- 400m
Shpejtesia mesatare e nyjes	0 – 25 metre/second?
Perioda e Simulimit	150 m
Simulation duration:	2 000 seconds

Simulimet:

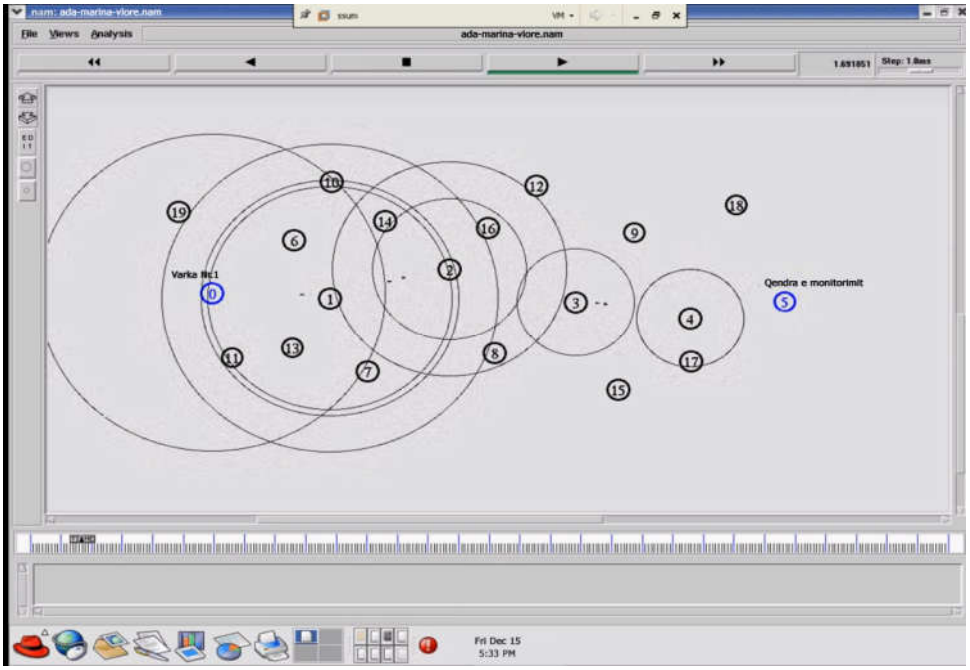
Simulim 1: Varka Nr 1 si pikë nisje dhe 5 si qendër monitorimi



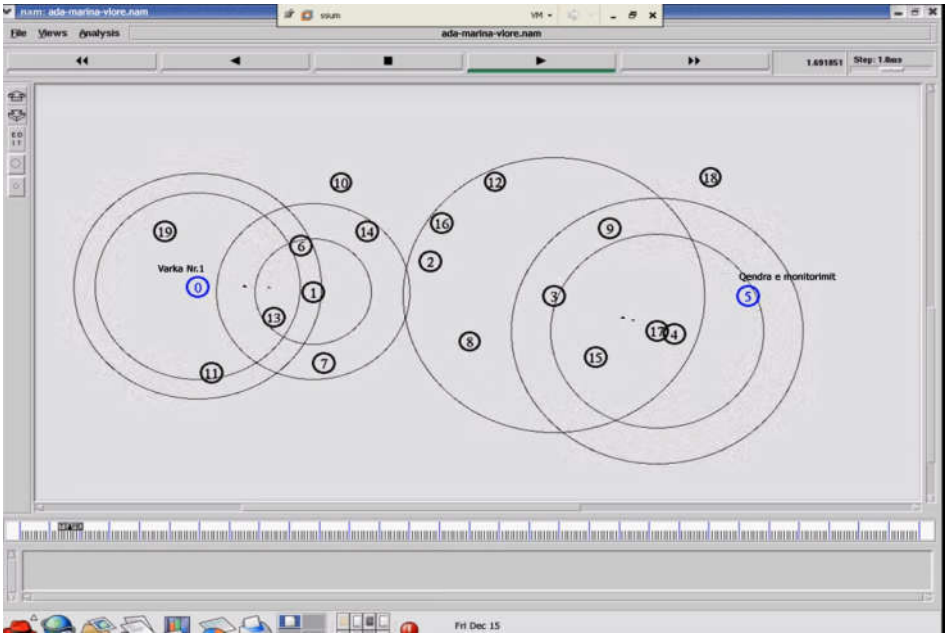
Simulim 2



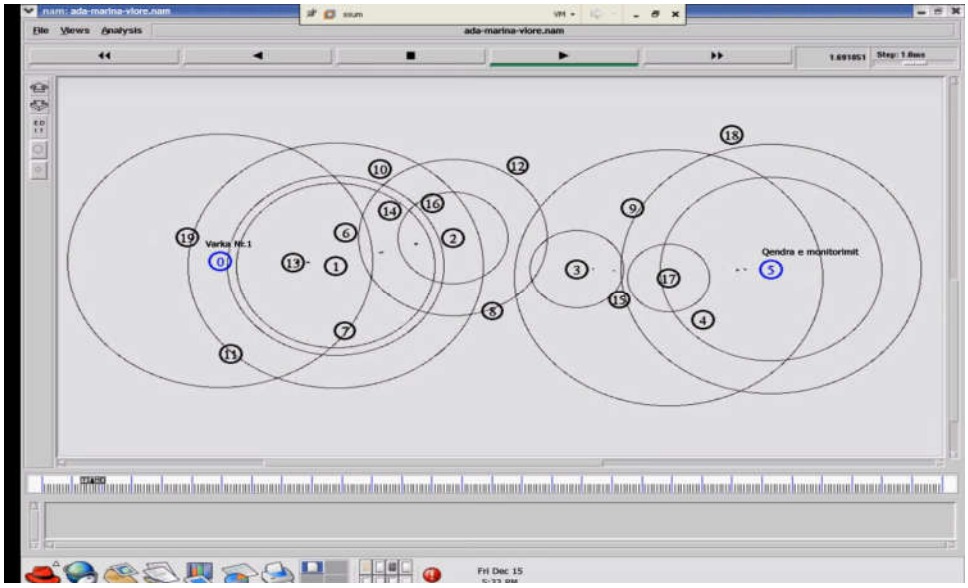
Simulim 3



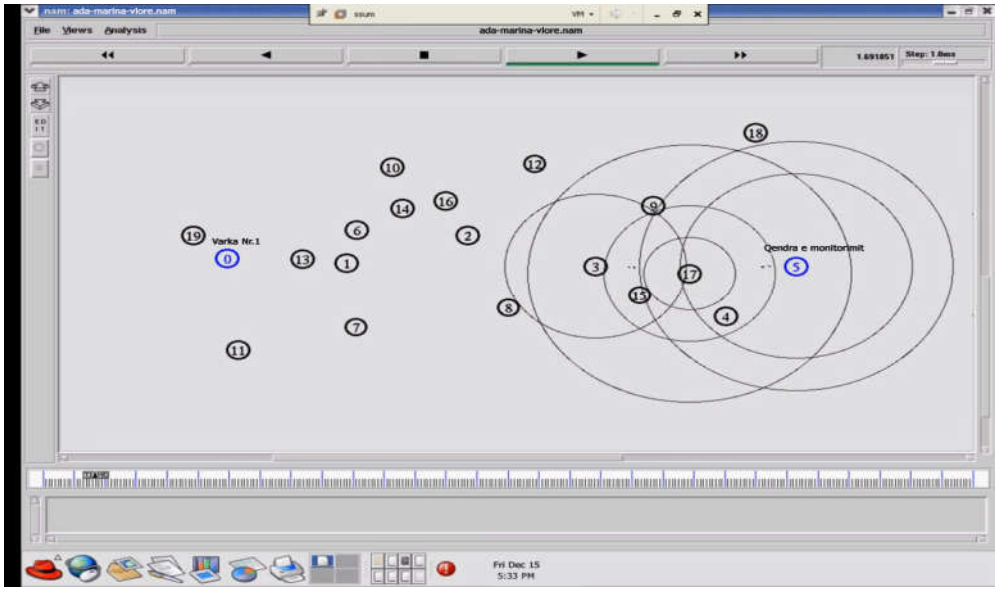
Simulim 4



Simulim 5



Simulim 6



4.2.4 Krahasimi i Protkollit InterNavComm me Protokolle të Tjera.

Gjatë këtij studimi ashtu siç mund të jetë vërejtur në përpjekje për të gjetur një protokoll më eficient dhe të sigurt na është dashur të studiojmë një sërë protokollesh të tjerë që përdoren shpesh në rrjetet ad hoc wireless të komunikimit. Tek kapitulli i parë ku kemi trajtuar protokollet e rrjeteve ad hoc wireless për komunikimet internavale, ndërsa në kap II dhe të III trajtuam sigurinë dhe tipet e ndryshme të protokolleve ad hoc wireless, në fund të kap.3 kemi kryer disa matje me 2 protokolle të ndryshme AODV dhe DSDR, me 2 simulator të ndryshëm MATLAB dhe DARS simulator, dhe nëpërmjet grafikëve dhe simulimeve të kryera kemi nxjerrë dhe konkluzionet përkatëse. Por duke qenë se protokolli ynë **InterNavComm** u realizua për tu përdorur në komunikimet ndër-navale mendojmë ta krahasojmë atë me **Flooding** algorithm pasi flooding/vërshimi ishte një nga teknikat e përdoruara në protokollet e komunikimeve ndër-navale për të cilat kemi folur në kapitullin e parë të këtij punimimi.

Flooding është një teknikë e zakonshme e përdorur shpesh për zbulimin e rrugëve dhe shpërndarjen e informacionit në wired dhe wireless rrjetat ad hoc. Strategjia e rrugëzimit është e thjeshtë dhe nuk bazohet në një mirëmbajtje të kushtueshme të topologjisë së rrjetit

dhe algoritma kompleks të rrugëzimit. Kjo mënyrë përdor një qajse reaktive ku secila nyje që merr data ose paketë kontrolli dërgon paketën te të gjithë fqinjët. Pas transmetimit një paketë ndjek të gjitha rrugët e mundshme.Vetëm në qoftë së rrjeti është i shkëputur, paketa do të gjejë destinacionin final. Ndërkohë që topologjia e rrjetit ndryshon transmetimi i paketës ndjek rrugë të reja.

Në figurën më poshtë konsiderojmë një vërshim/flood nga A; së pari arrin B përmes AB dhe E përmes AE. Më pas C përmbyt CD dhe CH; D përmbyt Dc; F përmbyt FG; G përmbyt GF, siç paraqitet tek fig. b

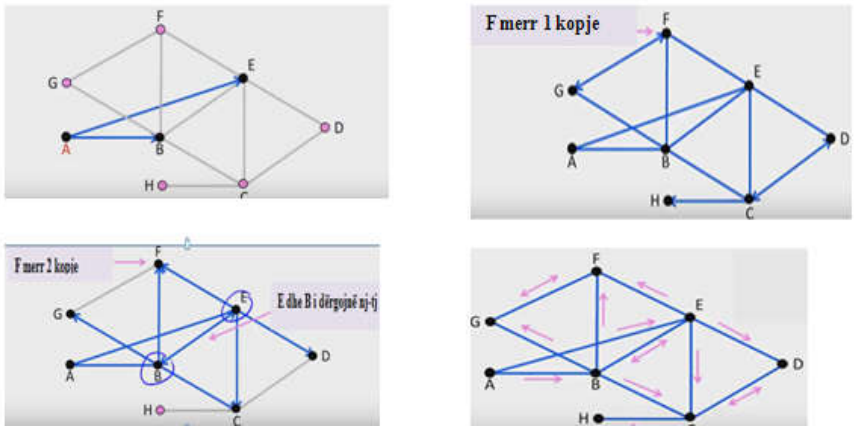


Figura 4.9. Paraqitja e Flooding nga A në H.

Nisemi nga B vërshon BC, BE, BF, BG dhe E përmbyt EB, EC, ED, EF. Ndërsa H nuk ka kë të vërshoje. Këtu mbaron vërshimi/flooding.

Flooding/përmbytja është forma më e thjeshtë në të cilën mund të ndodh që paketa të replikohet nga nyjet e rrjetit. Për të shmangur që një paketë të qarkullojë vazhdimisht në rrjet një fushë e cila përmban numërimin e hopeve përfshihët në paketë. Fillimisht numerimi i hopevë është vëndosur përafërsisht sa diametri i

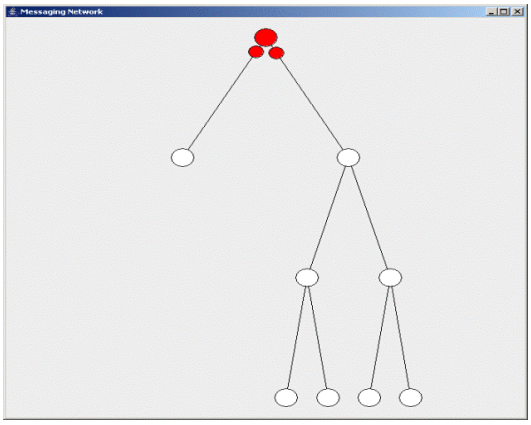


Figura 4.10. Simulim nga algoritmi i Flooding

rrjetit. Ndërkohë që paketa udhëton përgjatë rrjetit, numërimi i hopevë zvogëlohet me një për çdo hop që përshkruhet. Kur numërimi i hopeve arrin në zero paketa thjesht bëhet discard. Një efekt i ngjashëm mund të arrihet duke përdorur një fushe time to live, e cila rregjistron numrin e njësive të herëve që paketa është e lejuar të "jetojë" në rrjet. Në përfundim të kësaj kohe, paketa nuk dërgohet më. Flooding mund të përmirësohet në saj të identifikimit unik të paketave të të dhënave, duke detyruar çdo nyje të rrjetit ti bëjë drop të gjitha paketat që ajo tani më i ka drejtuar. Pavarësisht thjeshtësisë së rregullit të drejtimit të paketave dhe kostoja e ulët e mirëmbajtjes, kjo teknikë vuan një sërë të metash.

- Disavantazhi i parë i flooding është ndjeshmëria e tij ndaj implosionit të trafikut. Ky efekt i padëshiruar shkaktohet nga kontrolli i dyfishtë ose dërgimi i paketës së të dhënave pambarimisht te e njëjta nyje. Flooding është ineficient pasi një nyje mund të marrë kopje të shumëfishta të mesazhit.
- Disavantazhi i dytë është problemi i mbivendosjes, overlapping. Overlapping ndodh kur dy nyje që mbulojnë të njëjtën zonë dërgojnë paketa që mbajnë informacion të ngjashëm te e njëjta zonë.
- Disavantazhi i tretë dhe më serioz janë burimet e verbëra. Rregulli i thjeshtë i dërgimit që flooding përdor për të rrugëzuar paketat nuk merr në konsideratë kufizimet e energjisë të nyjeve sensor. Dhe kështu energjia e nyjes mund të konsumohet shpejtë, duke reduktuar ndjeshëm jetëgjatësinë e rrjetit.
- Disavantazh tjetër është edhe kompleksiteti I lartë, N^2.

InterNavComm: Për të adresuar rrugët më të shpejta në krahasim me Flooding, një qasje tjetër referuar si InterNavComm është propozuar, i cili është një derivim i protokollit flooding. I ngjashme me flooding, InterNavComm përdor një rol të thjeshtë të drejtimit dhe nuk kërkon një mirëmbajtje të kushtueshme të topologjisë ose algoritma kompleks të rrugëzimit.

Ndryshe nga flooding, ku një paketë data bëhet broadcast te të gjithë fqinjët, InterNavComm kërkon që secila nyje të dërgojë paketën e ardhur te nyja fqinjë rastësore. Algoritmi fillon me krijimin e infrastrukturës hierarkike virtuale. Nyjet e së njëjtës qelizë ose e qelizave fqinje, që janë brenda rrezes së komunikimit shkëmbejnë mesazhin fillestar "Përshëndetje". Si rezultat çdo nyjë e di pozicionin e të gjitha nyjeve që mund të komunikojnë me të. Në protokollin tonë procesi i update është njësoj si i rutimit gjeografik ndërkohë që nyjet lëvizin në të njëjtin drejtim dhe afërsisht me të njëjtën shpejtësi mesatare në vijë të drejtë. Intervali i update_imit varet nga lëvizshmëria e nyjes, nëse kjo lëvizshmëri është e lartë nevojitet një interval i shkurtër update. Kështu si përfundim për InterNavComm mund të thuhet se:

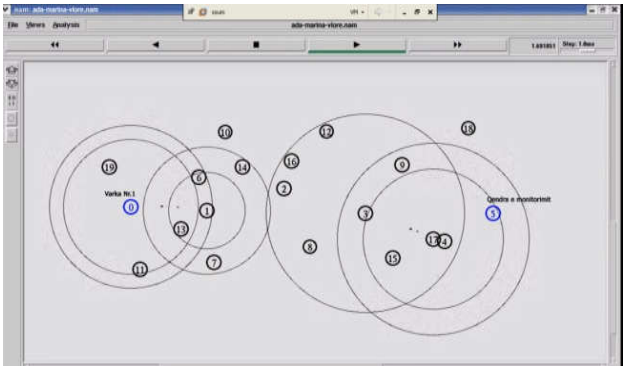


Figura 4.10. Simulim nga algoritmi InterNavComm

- Ky protokoll është i bazuar në rutimin gjeografik dhe ka një strukturë hierarkike, të organizuar në 3 nivele. Eleminon efektin negativë të stuhive të transmetimit.
- Mënjanon problemin e implosion/kolapsit duke reduktuar numri e paketave që secila nyje dërgon te fqinjët e vetë me një kopje.Vonesa që përjeton një paketë në rrugën e vetë drejt destinacionit mund/duhet të tejkalohet, veçanërisht në një rrjet të madh.
- Protokolli ynë përmirësonë cilësinë dhe besueshmërinë e komunikimeve ndërmjetore duke e mbajtur rrjetin pak të ngarkuar dhe është i vlefshëm edhe në situatat e emergjencës.
- Nëse kompleksiteti i flooding është N^2, kompleksiteti i protokollit tonë të rutimit është N+L, pra më i vogël, një sfidë e protokolleve të rutimit është ulja e kompleksitetit.

- Përdorimi i një strukture hierarkike rrit shkallëzueshmërinë (scalability), nga mënyra sesi performon tregon se rrit efektivitetin dhe sigurinë në komunikimet ndër-navale të emergjencës, breg- anije dhe anije me anije.

V. PËRFUNDIME & KONKLUZIONE

Në këtë punim të tezës jemi përpjekur që të merremi me çështjet e sigurisë në rrjetet ad hoc mobile(MANET). Por dhe me rritjen e sigurisë dhe eficiencës të komunikimit në portet e vogla të qytetit të Vlorës dhe jo vetëm por edhe në të gjithë portet e Shqipërisë.

Po pse morëm në studim rrjetet ad-hoc? Një rrjet mobile ad hoc ka natyrën e hapur të mjeteve të komunikimit dhe lëvizjen e lirë që është arsyeja pse ajo ka nevojë të jetë më tepër e prirur ndaj rreziqeve të sigurisë p.sh ndërhyrjet, shpalosjet e informacionit dhe mohimi i shërbimit etj. Një rrjet mobile ad hoc ka nevojë për nivel të lartë të sigurisë, krahasuar me rrjetet tradicionale me tel. Kështu në këtë temë u diskutuan karakteristikat e ndryshme të MANET dhe disa nga çështjet tipike dhe disa dobësi të rrezikshme në rrjetet mobile ad hoc. Qëllimi tjetër i kësaj çështjeje ishte diskutimi i aspekteve të ndryshme të sigurisë në MANET; së pari u diskutua mbi teknikat shumë-shtresore të zbulimit të ndërfutjes në rrjet in multi hop te MANET; së dyti u diskutuan problemet e sigurisë që lidhen midis rrjetit multi hop dhe nyjeve celulare në rrjet mobile ad hoc.

Më pas janë diskutuar disa nga llojet kryesore të sulmit të rrjetit të lëvizshëm ad hoc që është përdorur për të kërcënuar rrjetet. Ne gjithashtu arritën që të dimë se teknika e zbulimit të ndërhyrjes Multi-layer është e realizueshme në rrjetin multi-hop e MANET; përveç kësaj gjithashtu diskutuam probleme të ndryshme të sigurisë të cilat ndërlidhen ndërmjet rrjetit multi hop dhe nyjeve celular në rrjetin mobile ad hoc. Në fund, ne u morëm me protokollet e rutimit, sjelljen e ndërhyrësit dhe se si të merremi me ndërhyrësin dhe të implementojmë disa nga mekanizmat e sigurisë që mund të përdoren për të ndihmuar rrjetet mobile ad hoc nga kërcënimet e jashtme dhe të brendshme të sigurisë. Dhe si përfundim konkluduam se cili nga protokollet e rutimit është i përshtatshëm për mjedise të ndryshme, psh në qoftë se ne përdorim protokollin e përshtatshëm për një MANET, kështu i

vështirësohet një infiltruesi sulmi ndaj rrjetit. Si përfundim në bazë të vërejtjeve, rrjeti ad hoc wireless është zonë shumë e gjerë, në të cilën studiuesit mund të zbulojnë dhe të hetojnë gjërat e reja në çdo fushë.

Në këtë studim gjejmë studime krahasuese të rrjetit celular dhe rrjetit ad hoc, zonat e aplikimit të rrjetit ad hoc wireless, rrjetit mesh wireless, rrjetit sensor wireless, rrjeti hibrid wireless, skemën e medium access e ad hoc rrjetit pa tel, rutimin në rrjetin ad hoc wireless, multicasting në ad hoc rrjet pa tel, protokollet shtresa transport e ad hoc rrjet pa tel, skema çmimi i ad hoc rrjetit pa tel, cilësia e shërbimit të rrjetit ad hoc wireless, vetorganizimin, sigurinë, menaxhimin e energjisë në rrjetin ad hoc wireless, përparimet e fundit në rrjetet wireless.

Rrjetet Ad Hoc të Automjeteve(VANETs) janë një teknologji e re dhe premtuese, kjo teknologji është një rajon i favorshëm për sulmuesit, të cilët do të përpiqen për të sfiduar rrjetin me sulmet e tyre keqdashëse. Ky dokument dha një analizë të gjerë për sfidat aktuale dhe zgjidhjet, dhe kritikat për këto zgjidhje, gjithashtu u propozua një zgjidhje e re që do të ndihmojë për të mbajtur një rrjet të sigurt VANET, në punën e ardhshme ne duam të zgjerojmë idenë tonë për certifikatat e mesazheve të sigurisë, si duhen krijuar, fshirë, dhe verifikuar dhe duke i verifikuar dhe testuar ato me anë të simulimit. Rrjetet e automjeteve jo vetëm që do të ofrojnë siguri dhe aplikacione për të shpëtuar jetën, por ata do të bëhen një mjet i fuqishëm komunikimi për përdoruesit e tyre.

Pas aksesimit të arkivave dhe dokumentacioneve reale të portit të Vlorës si dhe testimin e protokollit InterNavComm, ashtu si në fushat e tjera të kërkimit shkencor përdorëm simulimet. Gjithashtu si në analizë dhe në simulim u përdor krahasimi me protokolle të tjera ekzistues për komunikimet mjet me mjet.

Konkluzione:

- ✓ Në këtë kërkim shkencor, ne paraqesim një skemë të re të rutimit, protokollin InterNavComm, i cili ofron një zgjidhje efikase, të shkallëzuar. InterNavComm dëshmon të jetë një zgjidhje fleksibile në sfidën e mirëmbajtjes së rrugëzimeve të sakta në rrjetet ad hoc wireless.

- ✓ Pas matjeve dhe simulimeve të kryera, themi se protokolli ynë InterNavComm performon më mirë se protokolle të tjera që përdorin teknikën Flooding. Skema hierakike e përdorur prej këtij protokolli bën të mundur implementimin e një politike ndryshe të shpërndarjes(të mesazheve), duke dhënë një shërbim të diferencuar dhe duke përmirësuar QoS(rëndësia e të cilit është përmendur në kapitujt e këtij punimi). InterNavComm mënjanon problemin e implosion/kolapsit duke reduktuar numri e paketave që secila nyje dërgon te fqinjët e vetë me një kopje Ky protokoll mundëson një komunikim në kohë reale midis distancës së varkave dhe varkave antarë të grupit. Gjithashtu mund të nxjerrim si konkluzion se protokollet e bazuar në topologji reaktive janë më të mirë se protokollet e rutimit të bazuar në topologji proaktive. Dhe protokolli ynë, InterNavComm bënë pjesë në protokolle të bazuar në topologji proaktive.
- ✓ Nëse kompleksiteti i flooding është N^2, kompleksiteti i protokollit tonë të rutimit është N+L, pra më i vogël, një sfidë e protokolleve të rutimit është ulja e kompleksitetit.
- ✓ Ky protokoll përmirëson cilësinë e komunikimeve pikë me pikë dhe është i vlefshëm edhe në situatat e emergjencës.
- ✓ Përdorimi i një strukture hierarkike rrit shkallëzueshmërinë (scalability), nga mënyra sesi performon tregon se rrit efektivitetin dhe sigurinë në komunikimet ndër-navale të emergjencës, breg- anije dhe anije me anije.
- ✓ Nga studimi ynë duket qartë se nevoja e krijimit të aplikimeve të reja, të sigurta pra të besueshme ngrihet edhe në portet shqiptare, dhe implementimi i protokollit tonë të ri InterNavComm edhe në portin e Vlorës, ku është fokusuar më shumë studimi im, do të ndihmonte në plotësimin e mangësive ekzistuese sidomos në ato zona ku mbulimi valor është i ulët ose mungon fare(zonat: Karaburunit, midis Qeparoit dhe Borshit, etj...)
- ✓ Pavarësisht nga kufizimet, mundësitë që të ofron ky protokoll rutimi janë më të mëdha se ato që mund të ofrojnë protokolle te tjera. Me protokoll rutimit InterNavComm arrihet koha minimale e komunikimit me konsumin minimal të

burimeve të rrjetit, si dhe merret parasysh prezenca e zonave 'gri' përgjatë rrugës në të cilin mjeti lëviz.

Puna në të ardhmen: Megjithatë, në tezën tonë kemi pranuar se vlerësimi aktual për artin e zgjidhjeve së sigurisë wireless është thuajse ad hoc. Ka disa të meta të cilat duhet të përmirësohen dhe disa prej tyre janë dhënë më poshtë:

- Mungesa e mjeteve efektive analitike, veçanërisht në rast të vendosjes së rrjetit wireless në shkallë të madhe.
- Gjetja dhe bllokimi i një përdoruesi të autentifikuar, i cili fillon të humbasë sjelljet brenda rrjetit.
- Kompromiset shumëdimensionale midis forcës së sigurisë,
- Komunikimi i sipërm(overhead)
- Llogaritja e kompleksitetit
- Konsumi i energjisë,
- Edhe pse është arritur deri diku Shkallzueshmëria ende mbetet kryesisht e paeksploruar.

Duhet të zhvillohet një metodologji efektive vlerësimi dhe udhrrëfyese që ndoshta do të përdoret dhe do të ketë nevojë për përpjekje ndërdisiplinore nga komunitete të ndryshme kërkimore të cilat janë duke punuar në sistemet celular, cryptography, dhe rrjeteve wireless. Në rastin e sigurisë kalimtare multicast është ende një problem i hapur.

Konstatojmë se :

- Komunikimi efektive ndërmjet mjeteve rritet duke përdorur protokolle efektive rutimi.
- Nje algoritem i mire rutimi mund te shmang bllokimin e trafikut mbi te gjitha linjat.
- Sfida e të gjitha protokolleve adreson në drejtim të shkallëzimit (scalability) dhe efektivitetit. Dhe protokolli ynë i propozuar realizon pikërisht këtë.

- Përmirëson shfrytëzimin e rrjetit në krahasim me protokollet ekzistues per komunikimet anije-për-anije. Ky Protokoll mund të përdoret për të zbatuar shërbimet mobile të diferencuara dhe prioritizimin e mesazhit.
- Le të themi se rrjetat ad hoc janë të mirë- krijuar si një zonë praktike kërkimore. Kanë shumë aplikueshmëri.
- Një protokoll On-demand ofron shumë avantazhe
- AODV i përdor avantazhet si tek Distance-Vector dhe në On-demand
- AODV ka shance të mira për standartizimin.
- Rrjetat Ad hoc mund të vendosen në Internet dhe më pas të sigurojnë domain_et wireles
- Teknikat e autokonfigurimit të addresave janë mirë-përshtatur

SHTOJCA

MESAZH STANDART

I DËRGOHET KAPITENERISË SË PORTIT DREJPËRSËDREJTI OSE NËPËRMJET AGJENSISË 24 ORË PARA MBËRRITJES, VETËM PËR ANIJET QË KRYEJNË OPERACIONET E LARJES SË CISTERNËS ME NAFTË BRUTO GJATË OPERACIONIT TË SHKARKIMIT TË NGARKESËS.

STANDARD MESSAGE

TO BE SENT TO HARBOUR MASTER DIRECTLY OR VIA AGENT 24 HOURS BEFORE ARRIVAL

ONLY FOR SHIPS CARRYING OUT COW DURING DISCHARGE.

- EMRI I ANIJES
- ***SHIP'S NAME***
- *TONAZHI DWT*
- ***TONNAGE DWT***
- CILËSIA DHE SASIA E NGARKESËS QË DO TË SHKARKOHET
- ***QUALITY AND QUANTITY OF CARGO TO BE UNLOADED***
- CILËSIA DHE SASIA E NGARKESËS NË TRANZIT
- ***QUALITY AND QUANTITY OF CARGO IN TRANSIT***
- *DRAFT PËR-NE*-MES ANIJE
- ***DRAFT FORE-AFT-MID SHIP***
- ORA E MBËRRITJES
- ***TIME OF ARRIVAL***
- OPERACIONI I BALLASTIMIT NJËKOHËSISHT ME SHKARKIMIN OSE SHKARKIMI DO TË NDËRPRITET ____ ORE PËR BALLASTIMIN

- ***BALLASTING CONCURRENTLY WITH DISCHARGE OR DISCHARGE WILL BE STOPPED ____ HOURS FOR BALLASTING***
- ANIJA TEKNIKISHT EFICENTE PËR SHKARKIMIN E NGARKESËS PËR TË KRYER OPERACIONET E LARJES SË CISTERNËS ME NAFTE BRUTO (COW)
- ***SHIP TECHNICALLY READY TO UNLOAD CARGO AND TO CARRY OUT COW***
- SISTEMI I GAZIT INERT COW, I KONTROLLUAR DHE ME EFIÇENCË TË PLOTË
- ***INERT GAS AND COW EQUIPMENTS TESTED AND FOUND IN EFFICIENT WORKING CONDITIONS***
- KAPITENI DEKLARON QË CISTERNAT E NGARKESËS JANË INERTIZUAR E MBAJTUR NËN PRESION NORMAL
- ***MASTER DECLARES THAT CARGO TANKS ARE INERTED AND PRESSURIZED***
- KAPITENI DEKLARON QË CILËSIA E OKSIGJENIT E PRANISHME NË CISTERNAT GJATË KRYERJES SË OPERACIONIT TË COW, MBAHET MË POSHTË SE 5% E VOLUMIT
- ***MASTER DECLARES THAT OXYGEN IN TANKS DURING COW OPERATIONS WILL BE KEPT BELOW FIVE PERCENT BY VOLUME***
- ANIJA ËSHTË OSE NUK ËSHTË E PAJISUR ME NJË SISTEM TË MBYLLJES HERMETIKE PËR MARRJEN E KAMPIONEVE TË NGARKESËS (MOSTRAVE)
- ***SHIP IS/IS NOT EQUIPPED WITH VAPOUR LOCK SYSTEM FOR CARGO MEASURING AND SAMPLING***

KOMUNIKIMI ANIJE - TOKË

SHIP-SHORE COMMUNICATIONS

Kanali VHF Telefon

VHF Channel Telephone

Harbour Master

Portit të Vlore – 1

The Port

Përfaqësuesi i Terminalit

Port ***Representative***

_____

_____

Asistenti

Assistant

Piloti

Pilots

Rimorkiatori

Tugger

STACIONI I POMPAVE

BOOSTER STATIONS

_____

_____

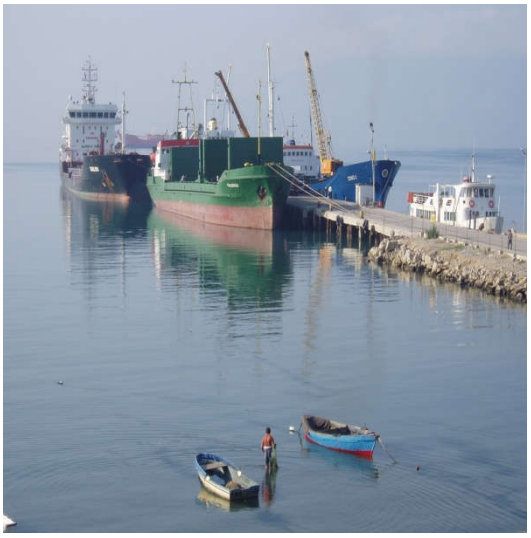
_____

_____

Njoftim për Motin

Weather **Report**

PAMJE NGA DISA PORTE TË VLORËS



PORTI I VJETËR,VLORË

PORTI TURISTIK I ORIKUMIT (I JAHTEVE)

PORTI RI,VLORË

I N S T R U K S I O N

PER VENDET E DYSHIMTA KU MUNDE TE KETE AKTIVITET TE KUNDRALIGJSHEM NEPERMJETE KUFIRIT BLU.

Grykderdhja e Lumit SEMAN 40 ^{0}52” 93’ N dhe **19^{0}24”** 24’ **E**

Grykderdhja e Lumit Vjose 40 ^{0}39” 01’N 19 ^{0}0 1” 03’ E

Hidrovori i AKERNIS 40^{0} 35” 65’ N 19^{0} 21”42, E

Hunda e Plakut ZVERNEC 40 32 85 N 19 22,65 E

TRIPORTE 40,29 85 19 N ,22 32. E

Ishulli SAZANIT 40 29 85 N 19 18 11 E

SHEN JANI 40, 26 41 N 19 19 92 E

SHEN JVASI 40 26 41 N 19 18 92 E

SHPELLA E HAXHIALIS 40 26 24 N 19 18 50. E

GJIRI I VARKES 40 24 68 N 19 17 89 E

GJIRI I ARUSHES 40 22 11 N 19 20 67 E

GJIRI I BRISTANIT 40 19 05 N 19,22 27. E

GJIRI I ANGLEZIT 40, 14 26 N 19,26 10 E

GJIRI I GRAMES 40 12 66 N 19 68 63 E

GJIU I DAFINES 40 11 40 N 19,31 06 E

Rruget e BARDHA 40,09 42 N 19,35 71 E

PORTO PALERMO 40, 03 02 N 19,26 93 E

BUNECI 39 56 39 N 19,56 04 E

BORSHE 40 02 25 N 19,51 43 E

KAKOME 39 55 58 N 19,56 58 E

SPILLE 40 05 70 N 19 44 74 E

GJIU I VLORES 40 26 19 N 19 23 94 E

Kanal Jug.Karaburun 40 27 76 N 87 19 17. E

Kanal Veri.Karaburun 40,31 54 N 19 15 99 E

RAGUZA 40 21 30 N 40 24 60 E

GJIRI I DUKATIT 40 20 53 N 19 26 16 E

UJI I FTOHTE 40 25 37 N 19 28 16 E

RADA VLORE 40 26 23 N 19 27 77 E

GJIRI I DURRESIT 41,15 91 N 19 24 89 E

RADA E PALLES 41 27 23 N 19, 21 38 E

Shenim: Keto te dhena jane mare nga manulai i lundrimit dhe jane te vleshme per efekt shpejteise ne kryerjen e veprimeve.

Misionii NJLTKM ne raste kur aktivizohen per kerkim shpetim.

Shërbimi i kërkim-shpëtimit ka për mision, të kryejë operacione të kërkim-shpëtimit në hapësirën tokësore dhe detare të RSH, në raste fatkeqësish të ndryshme, për të ndërhyrë, kërkuar, gjetur dhe shpëtuar persona të humbur ose të zhdukur, pra kur jeta njerëzore është në rrezik.

Per kerkim shpetimin ne dete

Roja Bregdetare ka përgjegjësinë e organizimit dhe realizimit të Operacioneve të veçanta në hapësirën detare.

Komponentët e shërbimit të kërkim-shpëtimit (SAR).

Sistemi i shërbimit të kërkimit dhe shpëtimit (SAR) si çdo sistem tjetër ka komponentët e tij, të cilët duhet të punojnë të gjithë së bashku për të siguruar funksionimin e sistemit. Zhvillimi i sistemit të kërkim-shpëtimit kërkon përcaktimin dhe ndarjen e rajoneve të kërkim-shpëtimit (SRR), në bazë të aftësive në marrjen e sinjaleve të rrezikut dhe të koordinimit e sigurimit të shërbimeve të kërkim-shpëtimit brenda këtyre rajoneve. Çdo rajon kërkim-shpëtimi (SRR) ka karakteristika unike si llojin e transportit, klima, topografia, kushtet fizike etj. Këto faktorë krijojnë lloje të ndryshme problemesh gjatë një operacioni kërkim-shpëtimi (SAR) në çdo rajon kërkim-shpëtimi (SRR). Faktorë të tillë influencojnë në zgjedhjen dhe përbërjen e shërbimeve, ambjenteve pajisjeve dhe stafit që kërkohet për çdo incident SAR.

✪ ***Detyrat kryesore.te NJLTKM ne operacionet e kerkim shpetimit.***

a.Të kryejë operacione kërkim-shpëtimi për të shpëtuar të mbijetuarit nga aksidentet dhe fatkeqësitë e ndryshme në tokë e në det;

b.Të kryejë operacione kërkimi-shpëtimi në ujërat territoriale për njerëzit dhe mjetet detare në rrezik;

c.Të kryejë operacione kërkim-shpëtimi të personave ushtarake e civile të humbur e në vështirësi në tokë e në det;

d.Të ndërhyjë për kërkimin dhe shpëtimin e jetës së njerëzve që janë në vështirësi në bashkëpunim me forcat e tjera dhe institucionet shtetërorë qendrore e lokale;

e.Të kërkojë dhe shpëtojë anijet e mbytura e mjetet në vështirësi (me persona në bord);

f..Të transportojë urgjent pranë spitaleve të sëmurë dhe të traumatizuar rëndë;

g.Të japë asistencë popullsisë së goditur nga fatkeqësitë natyrore.

h.Të bashkëpunojë me strukturat e kërkim-shpëtimit të vendeve kufitare dhe aleate mbi bazën e marrëveshjeve dhe konventave ndërkombëtare për kërkim-shpëtimin dhe ndihmën e njerëzve në rrezik, shtetas shqiptare ose të huaj, në territorin tokësor dhe në zonën e përgjegjësisë detare të Republikës së Shqipërisë;

i..Të marrë pjesë së bashku me autoritetet kompetente civile qendrore e lokale në operacionet e ndihmës, në aksidentet shumë të rënda katastrofat dhe fatkeqësitë natyrore, duke ndihmuar per te realizuar operacionet komplekse të kërkim-shpëtimit të strukturave tokësore, apo detare që përfshihen në to, duke përcaktuar përparësitë e ndërhyrjeve për shpëtim dhe ndihmë.

Përveç sistemeve të përshtatshme të lundrimit dhe radio- aparaturave të përdorshme, në bord të mjeteve detare duhet të jenë edhe këto pajisje:

- Një kopje listë të Kodit Ndërkombëtar të Sinjaleve.
- Një kopje të manualit I.M.C.O MERSAR
- Varka dhe mjete shpëtimi, pajisje e veshje nënujore
- Fenerë, llamba kuti ndriçuese e tymuese, fishekë zjarri etj.
- Radio mobile (UHF,VHF) , GPS,
- Ushqime të ndryshme dhe pije të ngrohta
- Dylbi (të zakonshme dhe me rreze infra), aparate fotografike, kamera

- Pajisje mjekësore të ndihmës shëndetësore për dhënien e ndihmës shumë personave në të njëjtën kohë.

Pajisjet e kerkim shpetimit.

Pajisjet e një mjeti kërkim-shpëtimi përveç pajisjeve normale që e bëjnë të mundshëm kryerjen e një operacioni kërkim-shpëtimi (aparaturat e përshtatshme për navigacion e radiokomunikim, vende komode për vrojtim, rezervuar karburanti ndihmës etj) duhet të jenë të gatshëm për përdorim dhe këto pajisje:

a. Dylbi;

b. Një kopje liste e kodit ndërkombëtar të sinjaleve:

c. Pajisje sinjalizuese, llamba, altoparlant, materiale piroteknike etj;

d. Radiostacione të mbartshme (VHF/UHF), kuti ndriçuese, kuti tymuese për përcaktimin e pozicionit të të mbijetuarve;

e. Paketa furnizimi me materiale të mbijetesës;

f. Fikse zjarri;

g. Aparate fotografik;

h. Pajisje shëndetësore të ndihmës shëndetësore;

i. Barela, pajisje për marrjen me vinç nga helikopteri, etj.

ANEKSI III

DETAJE TEKNIKE TË PAJISJEVE TË SINJALEVE ZANORE

1. Sirena

a. Distancat dhe frekuencat e dëgjimit të zërit

Frekuenca bazë e sinjalit do të shtrihet brenda intervalit 70-700 Hz.

Distanca e dëgjimit të sinjalit nga sirena do të përcaktohet nga ato frekuenca të cilat mund të përfshijnë frekuencat bazë dhe ose më të larta, të cilat shtrihen brenda intervalit 180-700

Hz (1 për qind) dhe të cilat japin nivele presioni të zërit të specifikuar në paragrafin 1(c) më poshtë.

b. Kufijtë e frekuencave bazë

Për të siguruar një shumëllojshmëri të gjerë të karakteristikave të sirenave, frekuenca bazë e një sirene do të jetë ndërmjet kufijve që vijojnë:

- 70-200 Hz për një anije me gjatësi 200 metra ose më shumë;
- 130-350 Hz për një anije me gjatësi 75 metra, por më pak se 200 metra;
- 250-700 Hz për një anije me gjatësi më të vogël se 75 metra.

c. Intensiteti i sinjaleve zanore dhe hapësira e dëgjimit

Një sirenë e montuar në anije në drejtimin e intensitetit maksimal të sirenës dhe në një distancë prej 1 metër nga ajo duhet të japë një nivel presioni zanor minimumi 1/3 e bandës oktave brenda hapësirës së frekuencave prej 180-700 Hz (1 për qind) të jo më pak se shifrave përkatëse të dhëna në tabelën më poshtë:

Gjatësia e anijes në metra	1/3 e nivelit të bandës oktave në 1 metër në dB referuar 2x10-5 N/m2	Distanca e dëgjimit në milje detare
200 ose më shumë	143	2
75 por më pak se 200	138	1.5
20 por më pak se 75	130	1
Më pak se 20	120	0.5

Distanca e dëgjimit në tabelën e mësipërme është për informacion dhe e përafërt me atë në të cilën një sirenë mund të dëgjohet në akset përpara anijes me probabilitet 90 për qind në kushtet e një ajri të pastër në bordin e anijes, duke pasur një mjedis mesatar niveli zhurme në vendet e dëgjimit (i marrë 68 dB në brezin e oktavës të përqendruar në 250 Hz dhe 63 dB në brezin e oktavës të përqendruar në 500 Hz).

Në praktikë distanca në të cilën mund të dëgjohet një sirenë është ekstremisht e ndryshme dhe varet në mënyrë kritike nga kushtet e motit; vlerat e dhëna mund të konsiderohen si tipike, por në kushtet e erës së fortë ose ambiente me nivel të madh zhurme në postet e dëgjimit mund të reduktohet shumë.

d. Pajisjet me drejtim

Niveli i presionit të zërit të një sirene me drejtim do të jetë jo më shumë se 4 dB poshtë nivelit të presionit zanor, në akset në çdo drejtim në planin horizontal brenda 45 gradëve nga aksi. Niveli i presionit zanor në çdo drejtim tjetër në planin horizontal do të jetë jo më shumë se 10 dB poshtë nivelit të presionit zanor në akset, kështu që distanca në të gjitha drejtimet do të jetë minimumi gjysma e distancës sesa në akset përpara. Niveli i presionit të zërit do të matet në atë të 1/3 të brezit të oktavës, e cila përcakton distancën e dëgjimit.

e. Pozicioni i sirenës

Kur duhet të përdoret një sirenë me drejtim si e vetmja sirenë në anije, ajo do të instalohet me intensitetin maksimal të drejtuar direkt përpara.

Një sirenë duhet të vendoset në anije praktikisht sa më lart të jetë e mundur, me qëllim të reduktimit të ndërhyrjes të zërave të emetuar, nga pengesa dhe gjithashtu të minimizojë rrezikun e dëmtimit të dëgjimit nga personeli. Niveli i presionit të zërit të sinjalit të vetë anijes në vendin e dëgjimit nuk duhet t'i kalojë 110 dB(A) dhe sa më shumë e praktikueshme nuk duhet të kalojë 100 dB(A).

f. Pajisja me më shumë se dy sirena

Nëse sirenat janë montuar në një distancë nga njëra-tjetra prej më shumë se 100 metra, ajo do të rregullohet në atë mënyrë që ato të mos lëshojnë sinjale spontane.

<u>Kuadri i komandimit</u>

Konsoli është bërë prej GRP dhe i montuar në një copë. Ajo është përshtatur për t'u vendosur në derën komunikuese të kabinës. Pozicioni i makinës është në anën e djathtë, ndërsa tastiera e radio- navigatorit është në të majtë.

Pamja e kuadrit të komandimit

Kuadri i komandimit të drejtuesit

Kuadri i komandimit të drejtuesit përfshin jo vetëm timonin, throttles, instrumentet e motorit dhe çelësat, por edhe çelësin e panelin për dritat, pompën e ËC-së, njësinë larëse-fshirëse, frëngjinë e kontrollit, busullën magnetike, ekranin AIS, Multi-funksional të ekranit FI-50, -33 RD, të dhënat e ekranit, ekosounder Humminbird dhe drita spot.

1. Ekrani Furuno FA-150 AIS	2. Dritë spot
3. Kompas magnetik	4. Humminbird 998CX, ekrani anësor echosounder
5. Ekrani Furuno RD-33 i organizimit të të dhënave	6. Ekrani Furuno FI-50 multi-funksional
7. Instrumentet e motorit (shikoni përshkrimin e hollësishëm më	8. Njësia e kontrollit të larje-fshirjes së xhamave të dritareve

poshtë)	(shikoni përshkrimin e hollësishëm më poshtë)
9. Paneli i çelësave (shikoni përshkrimin e hollësishëm më poshtë)	10. Throttles të motorit, kontrollet e trim dhe animit
11. Timoni	12. Çelësat e motorit

Ekrani Furuno FA-150, busull magnetike, drita spote, ekran Humminbird ekosounder. Shih manualin e ndërtuesit për instrumentet Furuno dhe Humminbird. Rreth Humminbird pamje 3D echosounder, ne kujtojmë se është e mundur të ruhet një sasi e madhe e të dhënave për një kartë shtesë SD (e cila aktualisht nuk është e disponueshme). Të dhënat e ruajtura mund të shfaqen duke përdorur software Humviewer të instaluar në laptopët e vënë në dispozicion.

Ekranet Furuno RD-33 and FI-50 (në krye)

Paneli i çelësave

Çelësat janë të ndarë në seksione. Secili është me etiketë dhe një LED me ngjyrë tregon se aplikimi është në funksion.

"Sirena" është një button që shtypet për të aktivizuar sirenën e instaluar në radar. Ventilatori është instaluar me qëllim që të shkarkojë avujt e benzinës të cilat mund të jenë të pranishme mbi depozitat, për shkak të avullimit të karburantit. Ventilatori (anti-ndezje, i llojit me motor) duhet të punojë për 4 minuta para fillimit OBM. Shih gjithashtu

procedurën "gati për të filluar" në fillim të këtij manuali dhe procedurën "Ndezja e motorit" në vijim.

Kur është e mundur, paralajmëroni njerëzit në bordin e varkës se është e nevojshme një ndalje emergjente.

Kuadri i komandimit të Radio-Navigatorit

Kuadri i komandimit të Radio-Navigatorit është në anën e majtë dhe përfshin të dy radiot VHF dhe UHF, tabelën Furuno, radar dhe të ekranit ekosounder me njësi të kontrollit dhe ekranit Navtex Furuno. Një dorezë është e montuar në tastierë për arsye sigurie. Tabela që është vendosur në mes të dy kuadrove të komandimit dhe e mbështetur nga dy prej tyre (varet nga kuadri i komandimit të majtë), kur nuk përdoret, qëndron e bllokuar vertikalisht, për ta bërë më të lehtë hyrjen në kabinën përpara. Tabela është prej alumini.

Mbi tastierë është vendosur një dritë spot, nën dritaren qendrore, për të ndriçuar tabelën në tryezë.

1. Ekran Furuno NAVTEX NX-300	2. Kuadri i komandimit i radios SEPURA
3. Radio SEPURA me altoparlantë	4. Ekrani multifunksional Furuno MU 155
5. Radio SEPURA me mikrofonin e parë	6. T&T RT5020 VHF radio me kufje
7. Njësia e kontrollit Furuno Navnet 3D	8. Dorezë mbajtëse
9. Socket 12V	

Mjeti lundrues është i pajisur me një tabelë të varur në tastierën e majtë. Ajo duhet të mbahet zakonisht e hapur, me tastierë në të djathtë dhe që përdoret për laptop, hartat detare, etj. Mbylleni atë (d.m.th. vendoseni atë në pozicion vertikal) vetëm kur keni nevojë për hyrje të qetë në kabinë dhe kur anija është e palëvizshme. Është e preferueshme të mos mbahet në këtë pozitë gjatë lundrimit se mund të jetë i rrezikshëm.

KUJDES

Gjatë lundrimit mos i mbani në tryezë tabelat e hartat në pozicion vertikal.

Tabela e hartës e vendosur në mes të kuadrit të komandimit. Copë plastike ose gome në tavolinë për të shmangur dëmet në tastierën e pilotit.

Bullon për të fiksuar tabelën e hartës në pozicion të hapur.

Mbështetëse e fiksuar ndërmjet dritares së majtë dhe asaj qendrore për t'u përdorur kur nuk është e nevojshme tabela e hartës ose kur duhet një akses

Radio Sepura me altoparlantë, ekran Navtex

Mikrofoni i parë Sepura dhe kufje T&T

Radio VHF T&T RT5020 dhe Furuno Navnet

Socket 12V

Poshtë kuadrit të komandimit, nënën e majtë, kutia e njësisë së kontrollit

Furuno HUB-101 i fiksuar te kabina.

Lidhja e PC (komjuter laptop) me Furuno Hub :Në qendër duhet të jetë i lidhur kablli i rrjetit që lejon të lidhë sistemin e Furuno në kompjuter portativ me softëare MaxSea. Ky program lejon të replikohen të gjitha kontrollet e anijes, të ngarkohen harta dhe rrugët, etj, të gjitha të dhënat e lundrimit dhe të varkës që vijnë nga instrumentet Furuno që mund të

Pozicioni i portës Ethernet për t'u përdorur për lidhjen e PC (hiqni kapakun)

Kablli i lidhur

shfaqen duke përdorur kartografi të softëare-it. Ajo do të bëjë gjithashtu të mundur ruajtjen e të dhënave, sipas procedurave të përcaktuara nga programi dhe do të jetë e mundur të shpëtojë vetëm imazhin e treguar nga ana e softëare në një kohë të dhënë duke përdorur procedurën shtyp në ekran - kopjo në aplikim (të tilla si Microsoft Office ® ® Ëord ®). Kjo pastaj do të jetë e mundur për të shtypur të dhënat e ruajtura.

Vini re se, kur lidhni kompjuterin portativ me sistemin, mund të shfaqet një mesazh paralajmërimi, edhe në qoftë se lidhja Ethernet është duke punuar siç duhet: kjo është për shkak të faktit se OS kërkon një lidhje interneti që, në të vërtetë, nuk është i pranishëm, por ky nuk është një mosfunksionim.

Parametrat e lidhjes: adresa I.P.: 172.31.3.150

Subnet mask: 255.255.0.0

KUJDES

Për të gjitha detajet në lidhje me përdorimin e Furuno, Humminbird, Mercury, T & T,: SEPURA, etj. instrumente, radio, softëare Maxsea, etj. ju lutem referojuni manualit

të / ndërtuesit / furnizuesit.

PORTI DURRËS:

Prioritetet kryesore të sigurisë për portin.

Siguria navigacionale në Portin e Durrësit garantohet nga: Sinjalistika detare (fenerët ndricues) e cila mbulohet nga Shërbimi Hidrografik Shqiptar dhe orienton drejt të gjitha anijet (mjetet lundruese) që i afrohen portit dhe radës së Durrësit për të shmangur përplasjet apo rënien në cekëtinë.

Të dhëna më të hollësishme mbi sa më sipër janë të pasqyruara në hartat navigacionale të cilat disponohen nga Shërbimi Hidrografik. Shërbimi i pandërprerë i monitorimit të trafikut detar në Kapitenerinë e Portit ka instruksion të detajuar mbi detyrat që duhet të kryejë gjatë komunikimit me anijet(mjetet lundruese) që i afrohen portit apo radës së Durrësit për ti orientuar në funksion të manovrave të sigurta për qëndrim në radë(spirancë)apo hyrje në port.

Nisur nga këto prioritete është bërë një ndarje më e detajuar si më poshte:

I. Facilitete , që duhet domosdoshmërisht të plotësojnë kodin ISPS,siç janë :
   - Terminali i konteinerëve
   - Terminali i trageteve

- Terminali shumëqëllimësh i kalatës perëndimore
- Terminali i mallrave rifuxho.
- Pontoni i karburantit

II. Facilitete dhe instalime , që nevojiten të përmirësohen duke qenë se konsiderohen pika të dobëta nga pikëpamja e sigurisë për operacione portuale por që nuk ndikohen nga kodi ISPS siç janë :
    - Porti në përgjithësi (hyrjet e portit , rrethimi i portit , ndricimi, dhoma e kontrollit të sigurisë etj).
    - Zonat e kufizuara , që nuk i përkasin faciliteteve të Portit që mund të jenë në përputhje me Kodin ISPS.
    - Zona e depozitave të karburantit
    - Kantieri Detar

III. Facilite dhe instalime që nuk përbëjnë pika të dobëta për operacionet portuale në përgjithësi dhe as preken nga Kodi ISPS , dhe për të cilat nuk janë propozuar masa specifike përmirësuese siç janë :
    - Porti i Peshkimit
    - Pjesa me e madhe e ndërtesave të administratës së autoritetit portual dhe facilitete të tjera .
    - Pjesa me e madhe e kompanive të vogla të vendosura në port.

Plani i sigurisë së Portit të Durrësit

Plani i sigurisë së Portit të Durrësit është aprovuar në 11 korrik 2007 , në të cilin është përcaktuar Niveli 1 i sigurisë detare për portin e Durrësit, është miratuar nga ministri i Transporteve dhe Telekomunikacionit

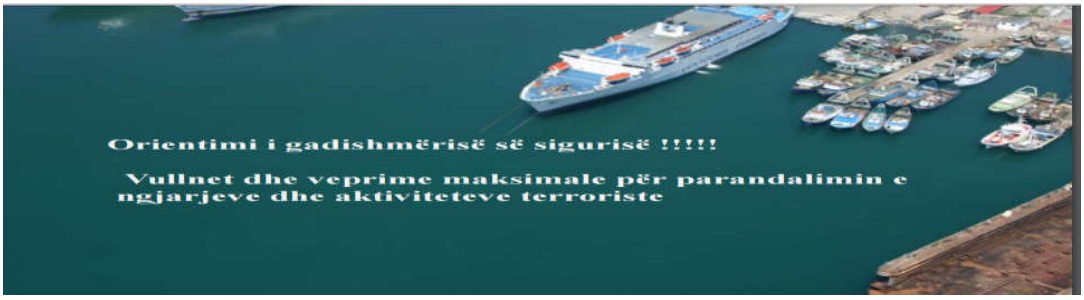
- Azhornimi i fundit i planeve të sigurisë është kryer nga oficeri i sigurisë së portit dhe janë miratuar nga Drejtori i APD-së në Janar 2012
- Plani i Sigurisë së Portit është përditësuar(çdo 1 vit) me ndryshimet infrastrukturore të kryera në Portin e Durrësit gjatë këtyre viteve.
- Eshtë aprovuar plani i emergjencave për Portin dhe hartuar plane rezerve dhe atyre të evakuimit, bazuar në kërkesat e kodit ISPS.

Zonat kryesore të sigurisë

Bazuar në planin e sigurisë janë përcaktuar 7 zona kryesore sigurie , ku secila prej tyre ka planin dhe oficerin e vet të sigurisë. Zonat e përcaktuara janë:

1. Porti në përgjithësi (zona e ngarkesave të përgjithshme dhe kalata lindore)
2. Terminal i konteinerëve
3. Terminal i trageteve
4. Porti i peshkimit . (që ndodhet brenda portit)
5. Kantieri detar
6. Depot e karburantit
7. Pontoni i karburanteve

Të gjitha zonat janë të rrethuara në përputhje me kërkesat e kodit ISPS dhe të pajisur me ndriçimin dhe sinjalistikën e nevojshme. Duke marrë në konsiderate punimet civile të rikonstruksionit në kalatën lindore , zona afër terminalit të trageteve (kalata 8) përdoret momentalisht për mallra rifuxho.



Të dhënat mbi trafikun në Portin e Durrësit ne vitet 2011 - 2015

Volumet e punës së APD-së për vitet si më poshtë					
PËRSHKRIMI	**2011**	**2012**	2013	2014	2015
TON TOTAL	**3.490.723**	**3.516.447**	**3.569.670**	**3.717.992**	**3.496.366**
EKSPORT	1.326.038	1.341.531	1.665.839	1.606.154	1.340.328
IMPORT	2.164.685	2.174.916	1.903.831	2.111.838	2.156.038
ANIJE TOTAL	**2.086**	**1.941**	**1.635**	**1.702**	**1.617**

Të dhënat mbi trafikun në Terminalin e Trageteve në vitet 2011 - 2015

Volumet e punës së APD-së për vitet si më poshtë					
PËRSHKRIMI	**2011**	**2012**	2013	2014	2015
TON TOTAL	**3.490.723**	**3.516.447**	**3.569.670**	**3.717.992**	**3.496.366**
EKSPORT	1.326.038	1.341.531	1.665.839	1.606.154	1.340.328
IMPORT	2.164.685	2.174.916	1.903.831	2.111.838	2.156.038
ANIJE TOTAL	**2.086**	**1.941**	**1.635**	**1.702**	**1.617**

BIBLIOGRAFIA

Jam mbështetur dhe kam ndjekur udhëzimet Chicago & APA(2001) përsa i përketë përdorimit të referencave në tekst.

Disa prej tyre:

- Andrew Tanenbaum, Computer networks.
- Jim Kurose, Computer Networks- A top down approach.
- Të dhëna të arshivuara të marra nga Marina: "Reparti Delta Forcë për kufirin dhe Migracionin Vlorë", Porti i Vjetër Vlorë dhe http://www.apdurres.com.al/(faqe kryesore për Portin e Durrësit).
- Mohamed Watfa "Survey of Routing Protocols in Vehicular Ad Hoc Networks" 2010, IGI Global.
- Simple AODV for MANET implementation and Source code in MATLAB, by Rupam
- H.Karl, A.Willing, "Protocols and Architectures for Wireless Sensor Networks".
- C. Siva Ram Murthy and B.S. Manoj " A text book on Ad Hoc Wireless Network architectures and protocols" Pearson Education 2013.
- E.Royer,Ch.K.Toh. A Review of Current Routing Protocols Ad Hoc Mobile Wireless Networks. IEE Personal Communication, Aprile 1999.
- Tom Seymour, Ali Shaheen :" History of Wireless Communication", Minot State University, USA , The Clute Institute, 2011.
- Charles E. Perkins and Elizabeth M. Royer. Ad-Hoc On-Demand Distance Vector Routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pages 90–100, New Orleans, LA, February 1999.
- Fan Li and Yu Wang, "Vehicular Ad HocNetworks: A Survey" , IEEE Vehicular Technology Magazine, June 2007
- J. Jubin and J. Tornow, "The DARPA Packet Radio Network Protocols," Proc. /E€€, vol. 75, no. 1, 1987, pp, 21-32.

- David B. Johnson and David A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In Tomasz Imielinski and Hank Korth, editors, Mobile Computing, volume 353, pages 153–181. Kluwer Academic Publishers, 1996
- L.R.Ford Jr. And D.R.Fulkerson, Flows in Networks, Princenton Univ. Press, 1962
- K. Sohraby, D.Minoli And T.Znati, "Wireless Sensor Networks Technology, Protocols and Applications", John Wiley & Sons New York 2007
- Mihail L. Sichitiu, Maria Kihl "Inter-Vehicle Communication Systems:A Survey" , IEEE Communications Surveys & Tutorials • 2nd Quarter 2008
- S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and App. 1.. Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97.
- L.Kleinrock and K.Stevens,"Fisheye: A Lenslike Computer Display Transformation," Technical report, UCLA, Computer Science Department, 1971.
- K. Sohraby ,D. Minoli And T. Znati ,"Wireless Sensor Networks Technology, Protocols,and Applications". John Wiley & Sons, New York, 2007.
- H. Karl ,A. Willig ,"Protocols and Architectures for Wireless Sensor Networks". John Wiley & Sons, New York, 2005 Jaya Bhatt, Naveen Hemrajani, "Effective Routing Protocol (DSDV) for Mobile Ad Hoc Network " International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013.
- Muhammad Arshad Ali &Yasir Sarwar "Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions", Computer Science Thesis no: MCS-2011-11 March 2011.
- M.Durresi, A.Durresi, L.Barolli. Hierarchical Communications for Battlefields. 21st International Conference on Advanced Information Networking and Applications Workshops, 2007 IEEE.
- M.Durresi, A.Durresi, L.Barolli. Optimized Geographical Routing Protocol for Vehicle Communications. Proceedings of the 25th IEE International Conference on

Distributed Computing System Workshops, 2005. International Conference on Advanced Information Networking and Applications Workshops, 2007.

- A. Sugikawa, Y. Morioka, K. Iwamura, Y. Tajika and M. Nakamura, "A computerized support system for nomadic collaboration", in Proceedings of MoMuC2: Second International Workshop on Mobile Multi-Media Communications, April 1995.
- Anu Chaudhary, K.K Gautam, Nirbhay Ahlawat "Effect of Cross Layer optimization of Traffic Management in Ad HOC Mobile Network", (IJCSIS) International Journal of Computer Science and Information Security,Vol. 12, No. 4, April 2014
- Soufiene Djahel, Ronan Doolan, Gabriel-Miro Muntean, and John Murphy "A Communications-Oriented Perspective on TrafficManagement Systems for Smart Cities: Challengesand Innovative Approaches", IEEE Communication Surveys & Tutorials, Vol. 17, No. 1, First Quarter 2015.
- K.Prasanth, Dr.K.Duraiswamy, K.Jayasudha, and Dr.C.Chandrasekar, "Improved Packet Forwarding Approach In Vehicular Ad Hoc Networks Using Rdgr Algorithm", International Journal of Next Generation Network (IJNGN), Vol.2, No.1, March 2010