REPUBLIKA E SHQIPËRISË
UNIVERSITETI POLITEKNIK I TIRANËS
FAKULTETI I TEKNOLOGJISË SË INFORMACIONIT
DEPARTAMENTI I ELEKTRONIKËS DHE TELEKOMUNIKACIONIT

MIRJETA ALINCI

PËR MARRJEN E GRADËS
"DOKTOR"
NË "TEKNOLOGJITË E INFORMACIONIT DHE KOMUNIKIMIT"
DREJTIMI "TELEKOMUNIKACION DHE INXHINIERI INFORMACIONI"

DISERTACION

NJË SISTEM I SIGURTË NË RRJETAT MOBILE AD-HOC BAZUAR NË FUZZY LOGIC

Udhëheqës Shkencor

Prof. Asoc. VLADI KOLIÇI

Tiranë, 2016

NJË SISTEM I SIGURTË NË RRJETAT MOBILE AD-HOC BAZUAR NË FUZZY LOGIC

Disertacioni

i paraqitur në Universitetin Politeknik të Tiranës

për marrjen e gradës

"Doktor"

në

"Teknologjitë e Informacionit dhe Komunikimit"

drejtimi Telekomunikacion dhe Inxhinieri Informacioni

nga

Znj. Mirjeta Alinci

2016

Udhëheqës Shkencor

Prof. Asoc. VLADI KOLIÇI

Juria

I aprovuar nga

_____, Kryetari i Jurisë së Disertacionit të Doktoraturës

_____, Anëtar i Jurisë së Disertacionit të Doktoraturës

_____, Anëtar i Jurisë së Disertacionit të Doktoraturës

_____, Anëtar i Jurisë së Disertacionit të Doktoraturës

_____, Anëtar i Jurisë së Disertacionit të Doktoraturës

I pranuar nga

_____,Dekan, Fakulteti i Teknologjisë së Informacionit

Miratuar nga

PËRMBAJTJA

LISTA E FIGURAVE ..... **I**

LISTA E TABELAVE ..... **II**

FALENDERIME ..... **IV**

ABSTRAKT **1**

PËRMBLEDHJE **2**

KAPITULLI I **4**

1.1 Hyrje 5

1.2 Punime të deritanishme 7

1.3 Motivimi i punimit 9

1.4 Qëllimi dhe kontributi i punimit 10

1.5 Struktura e disertacionit 12

KAPITULLI 2 RRJETAT MOBILE AD HOC (MANET) **13**

2.1 Hyrje 13

2.2 Karakteristikat e rrjetave MANET 14

2.3 Rrugëzimi në MANET 16

2.3.1 Protokollet Proaktivë në rrjetat MANET 17

2.3.1.1 Rrugëzimi sipas gjendjes së linjës i optimizuar (OLSR) 18

2.3.1.2 Vektori distancë hap pas hapi (DSDV) 18

2.3.2 Protokollet reaktivë 19

2.3.2.1 Vektori distancë sipas kërkesës (AODV) 20

2.3.2.2 Rrugëzimi i burimeve dinamike (DSR) 20

2.3.2.3 Algoritmi i rrugëzimit përkohesisht i rregulluar-TORA 21

2.3.3 Protokollet Hibridë 22

2.3.3.1 Protokolli i rrugëtimit në zona (ZRP) 22

2.3.4 Clustering në MANET 23

2.3.5 Protokollet e rrugëzimit të bazuar në Cluster 24

2.3.5.1 Algoritmi clustering d-Hop i bazuar në lëvizshmëri(MobDHop) 24

2.3.5.2 Algoritmi clustering i bazuar në parashikimin e lëvizshmërisë (MPBC) 25

2.3.5.3 Algoritimi me CH me afërsi ndërmjet tyre 3 hop (3-hBAC) 25
2.3.5.4 Algoritmi clustering me ID lidhjeje k-hope (KCONID) 25
2.3.5.5 Algoritmi i ruajtjes së energjisë i bazuar në rritjen e cluster-it (ECEC) 26
2.3.5.6 Algoritmi Max-Heap Tree i bazuar në efiçencën e energjisë..... 26
2.3.5.7 Algoritmi clustering bazuar në ngarkesë (WCA)..... 27
2.3.5.8 Algoritmti clustering i bazuar në ngarkesën fleksibël (FWCA) 27
2.4 Aplkimet e MANET 27
KAPITULLI 3 SIGURIA NE MANET 29
3.1 Hyrje 29
3.2 Aspekte të sigurisë 30
3.3 Kërcënimet ndaj rrjetave MANET 33
3.3.1 Kufizimet dhe kërcënimet në rrugëzimin bazuar në clustering..... 40
3.4 Mekanizmat e sigurisë 42
3.5 Siguria e rrugëzimit në MANET 43
3.5.1 Protokoll i sigurtë ad hoc (SAR) 44
3.5.2 Protokoll rrugëzimi vector distance efikas i sigurtë SEAD 44
3.5.3 Protokoll i sigurtë sipas kërkesës për MANET (ARIADNE) 45
3.5.4 Rrugëzim i autentikuar për rrjetat ad hoc (ARAN)..... 45
3.5.5 Dedektimi, parandalimi dhe reagimi i AODV 46
3.5.6 Bashkëpunimi i nyjeve: Drejtësia në MANET Dinamik (CONFIDANT).... 46
3.5.7 Protokoll i sigurtë ad hoc me ndihmën e pozicionit (SPAAR) 47
3.5.8 AODV bazuar në metodën e autentikimit kriptografik (SAODV) 47
3.5.9 Protokoll eficient rrugëzimi bazuar në vendndodhjen anonime (ALERT)... 48
3.5.10 Protokoll rrugëzimi i besueshëm bazuar në cluster (CBTRP) 48
3.5.11 Protokoll i sigurtë rrugëzimi bazuar në clustering i orientuar nga besueshmëria (STACRP) 49
3.5.12 Siguria e algoritmit clustering bazuar në ngarkesë (SCA)..... 49
3.5.13 Një cluster i sigurtë në MANET duke përdorur algoritmin Frd..... 50
3.5.14 Algoritmi i zgjedhjes së CH bazuar në lidhjen Fuzzy (FRCA)..... 50

KAPITULLI 4 FUZZY LOGIC 51
4.1 Hyrje 51
4.2 Kuptimi i Logjikës Fuzzy 52
4.2.1 Thelbi i logjikës fuzzy 54
4.3 Bazat e teorisë së Fuzzy set 55
4.3.1 Kuantifikimi i paqartësisë 56
4.3.2 Përkufizimet e fuzzy set 57
4.3.3 Variablat gjuhësorë 61
4.4 Kontrolli Fuzzy 62
4.4.1 Kontrolleri Fuzzy logic 63
4.5 Fuzzification 64
4.5.1 Funksionet e anëtarësimit 65
4.5.2 Karakteristikat e Funksionit të Anëtarësimit 67
4.5.3 Përcaktimi i vlerës së anëtarësimit 68
4.6 Defuzzification 69
4.6.1 Metoda e defuzzification Tsukamoto 69
4.6.2 Metoda e qendrës së zonës (COA) 70
4.6.3 Metoda e mesit të maksimumit (MOM) 70
4.6.4 Defuzzification ku dalja e rregullave është funksion i hyrjes 71
4.7 Sistemi Fuzzy i bazuar në rregulla 71
4.7.1 Formimi i rregullave 71
4.7.2 Sistemi i inference fuzzy (FIS) 72
4.7.3 Funksionimi i sistemit inference fuzzy 72
4.8 Metodat e fuzzy inference 74
4.8.1 Metoda Mamdani 74
4.8.2 Metoda Tagaki- Sugeno 75
4.8.3 Krahasimi ndërmjet metodës Mamdani dhe Sugeno 76
4.10.2 Rregullat e kontrollit Fuzzy 77
4.9 Baza e njohurive të kontrollit 78

4.10 Marrja e vendimeve fuzzy 80
KAPITULLI 5 SISTEMET E PROPOZUAR..... 81
5.1 Aplikimi i fuzzy logic për kontroll 82
5.2 Sistemi i propozuar 1 (F2SMC 1) 83
5.3 Procedura më vlerësimin e besueshmërisë së nyjeve cluster 89
5.4 Rezultatet eksperimentale për sistemin F2SMC 1 92
5.5 Sistemi i propozuar II (F2SMC 2) 97
5.6 Rezultatet eksperimentale për sistemin F2SMC 2 102
5.7 Krahasimi i dy sistemeve të propozuar 103
PËRFUNDIME 108
1. Përfundime për punimin 108
2. Objektiva në të ardhmen 109
LISTA E SHKURTIMEVE 110
LITERATURA..... 114

LISTA E FIGURAVE

Figura 2.1. Një rrjet moble Ad hoc 13
Figura 2.2. Protokollet e rrugëzimit në MANET 16
Figura 2.3. Clustering në MANET 23
Figura 3.1. Sulmet e jashtëm dhe të brendshëm 34
Figura 3.2. Sulmet aktivë dhe pasivë 35
Figura 4.1. Niveli “i gjatë” 57
Figura 4.2. Fuzzy subset A 58
Figura 4.3. Funksionet e anëtarësimit për “i shkurtër”, “rreth mesatar”, “i gjatë” 60
Figura 4.4. Diagram bllok e FLC 64
Figura 4.5. Funksioni i anëtarësimit 67
Figura 4.6. Modeli i sistemit inference 73
Figura 5.1. Modeli i sistemit F2SMC 1 83
Figura 5.2. Funksioni i anëtarësimit për parametrat e hyrjes dhe daljes 86
Figura 5.3. Bllokskema e procedurës për përcaktimin e besueshmërisë së nyjeve 89
Figura 5.4. Dalja e sistemit F2SMC 1 për NNC të ndryshëm 91
Figura 5.5. Modeli i sistemit F2SMC 2 92
Figura 5.6. Funksioni i anëtarësimit për parametrat e hyrjes dhe daljes 95
Figura 5.7. Lidhja ndërmjet parametrave të hyrjes dhe daljes për sistemin F2SMC 2 .. 102
Figura 5.8. Krahasimi i dy sistemeve për NNC=0.1 njësi 104
Figura 5.9. Krahasimi i dy sistemeve për NNC=0.5 njësi 105
Figura 5.10. Krahasimi i dy sistemeve për NNC=0.9 njësi 106

LISTA E TABELAVE

Tabla 5.1. Tabela e rregullave fuzzy për F2SMC 1 87
Table 5.2. Tabela e rregullave fuzzy për F2SMC 2 96

FALENDERIME

Së pari, falenderoj përzemërsisht dhe shpreh mirënjohjen time të veçantë për udhëheqësin shkencor Prof. Asoc Vladi KOLIÇI pa ndihmën dhe kontributin e të cilit nuk do të mund të mbyllej me sukses ky punim.

E falenderoj Prof. Asoc. Vladi KOLIÇI dhe në cilësinë e Dekanit të Fakultetit të Teknologjisë së Informacionit për pozitivitetin dhe mbështjen.

Falenderoj përgjegjësin e departamentit Prof. Asoc. Algenti LALA për bashkëpunimin dhe përkrahjen e vazhdueshme.

Falenderoj gjithë kolegët e departamentit të Elektronikës dhe Telekomunikacionit për mbështjetjen e vazhdueshme dhe në veçanti Dr. Evjola Spaho.

Falenderoj familjen time e cila më ka mbështetur gjatë gjithë kohës.

Mirjeta Alinci

ABSTRACT

The Mobile Ad hoc Networks (MANETs) are gaining popularity in recent years due to their flexibility and they can be deployed at any location without pre-existing infrastructure. They are used in various contexts such as collaborative, military application or in emergency services. In these types of networks each device works as host/router and are reconfigurable. Hence it is confronted with many challenges, such as the mobility of hosts, the dynamic topology, the multi-hop nature in transmission, the limited bandwidth and battery, security. To enhance the effectiveness of the network and to avoid routing problems such as overload, clustering techniques is used in MANET. Clustering increases the lifetime of routes, scalability and reduces congestion because the routes between clusters designates in advance.

Unique features of MANET like flexibility, dynamic topology, the mobility of nodes and lack of infrastructure make these networks more vulnerable to various attacks. Since these networks placed in the open environment where all nodes act together in sending packets on the network, malicious nodes is difficult to detect. So it is difficult to build a secure protocol compared with wired networks or those based in infrastructure. To ensure reliable communication in different environments, the main concern in MANET is the security of basic operations of the network.

That is fundamentally a difficult challenge to ensure communication and maintaining connection of nodes in the presence of malicious nodes in a topology changing multihop wireless network.

In this work we propose two systems based on fuzzy logic for improving the reliability of cluster nodes in MANETs. Based on Fuzzy logic controller determine for each node in cluster if it’s reliable to remain in the cluster (to participate in the transmission of packets). If it’s not reliable the node leave from cluster (do not participate in the transmission of packets).

PERMBLEDHJE

Rrjetat e Lëvizshme Ad hoc (MANET) kanë fituar popullaritet në vitet e fundit për shkak të fleksibilitetit të tyre dhe mund të vendosen në vende pa ndonjë infrastrukturë egzistuese. Këto rrjeta përdoren në kontekste të ndryshme si aplikime ushtarake ose shërbime të emergjencës. Në këto tipe rrjetash çdo pajisje punon si host / router si dhe mund të rikonfigurohen vetë. Ndaj këto rrjeta përballen me disa sfida si lëvizshmëria e hosteve, topologjia dinamike, gjerësia e brezit dhe bateria e kufizuar, siguria. Për të rritur efektivitetin e rrjetit dhe për të shmangur problemet e rrugëzimit si mbingarkesa, përdoret teknika clustering në MANET. Clustering rrit jetëgjatësinë e rrugëve, shkallëzueshmërinë dhe ul mbingarkesën duke qenë se rrugët ndërmjet cluster-ve caktohen paraprakisht.

Karakteristikat unike të MANET si fleksibiliteti, topologjia dinamike, lëvizshmëria e nyjeve dhe mungesa e infrastrukturës i bëjnë këto rrjeta mjaft të cënueshëm nga sulme të ndryshëm. Meqenëse këto rrjeta vendosen në mjedis të hapur ku të gjitha nyjet bashkë veprojnë në dërgimin e paketave në rrjet, nyjet me qëllim të keq është e vështirë të zbulohen. Ndaj është e vështirë të ndërtohet një protokoll i sigurtë krahasuar me rrjetat me tel ose ato të bazuar në infrastrukturë. Për të siguruar komunikim të besueshëm në mjedise të ndryshëm, shqetësimi kryesor i rrjetave MANET është siguria e veprimeve bazë të rrjetit.

Është një sfidë e vështirë të sigurohet komunikimi dhe mbajtja e lidhjes në prani të nyjeve me sjellje të keqe në një topologji rrjeti pa tel multihop të ndryshueshëm vazhdimisht.

Në këtë punim propozohen dy sisteme të bazuar në logjikën Fuzzy për përcaktimin e besueshmërisë së nyjeve cluster në MANET. Duke u bazuar në kontrollerin logjik fuzzy përcaktohet për çdo nyje në cluster nëse është e besueshme të mbetet në cluster (të marrë pjesë në transmetimin e paketave). Nëse nuk është e besueshme nyja largohet nga cluster (përjashtohet nga procesi i transmetimit të paketave).

KAPITULLI 1
HYRJE

1.1 Punime të deritanishme

Në këtë seksion përfshihet një analizë e punimeve kërkimore shkencore e viteve të fundit në fushën e sigurisë së MANET, duke u fokusuar më konkretisht në sigurinë e rrugëzimit në MANET.

Natyra e decentralizuar e MANET, lëvizshmëria e nyjeve, mungesa e infrastrukturës fikse i bën këto rrjeta mjaft të pambrojtur ndaj sulmeve të ndryshëm. Pra siguria në këto rrjeta është një sfidë e vështirë.

Në MANET është e lehtë për sulmuesit të futen ose të lënë rrjetin dhe të përgjojnë atë, duke qenë se nuk ka lidhje fizike. [13]

Pa vendosjen e një skeme sigurie, një nyje e jashtme mund të pretendojë të bëhet një nyje e brendshme dhe të marrë pjesë në rrugëzimin e paketave, ngatërrimin e tyre, injektimin e paketave false ose mbingarkesën e rrjetit.

Në literaturë gjendet një numër i madh studimesh në lidhje me mekanizmat e sigurisë së rrugëzimit kundrejt sulmeve sipas kërkesave të ndryshme të sistemit në MANET. Vetëm procedurat e rrugëzimit nuk mund të garantojnë dërgimin e sigurtë dhe të pashqetësuar të të dhënave përmes rrjetit.

Teknikat konvencionale të tilla si autentikimi, kontrolli i aksesit, enkriptimi dhe nënshkrimi dixhital përbëjnë linjën e parë të mbrojtjes ose sistemet e bazuar në besueshmëri. Këtu përfshihen:

Multicasting i sigurtë: Eshtë një metodë ku një paketë të dhënash mund të transmetohet nga një dërgues dhe të kopjohet nga një grup marrësish.

Rrugëzimi i sigurtë: Shumica e protokolleve të rrugëzimit në MANET janë të pambrojtur nga sulmet që mund të ngrijnë gjithë rrjetin. Nevojiten disa zgjidhje që të funksionojë rrjeti.

Rrugëzimi i fshehtë: Ndërtohen protokolle të sigurtë që privojnë nyjet e ndërmjetme nga analiza e trafikut

Menaxhimi i çelësit: Siguria në MANET arrihet kryesisht nëpërmjet Autoritetit të Certifikatës së Besuar (CA). CA e kompromentuar mund të dëmtojë lehtë gjithë rrjetin.

Si linjë e dytë e mbrojtjes janë implementuar në MANET sistemet e dedektimit të ndërhyrjeve dhe mekanizma të përforcimit të bashkëpunimit që ndihmojnë në mbrojtjen kundër sulmeve.

1.1.1 Sistemet e bazuar në besueshmëri

Fillimisht llogarisin vlerën e besueshmërisë duke përdorur informacion të tillë si numri i paketave të dërguara dhe numri i paketave për t'u dërguar. Vlera e besueshmërisë është raporti i paketave të marra me numrin e paketave të dërguara dhe varet nga fqinjët. Kjo vlerë pastaj krahasohet me një vlerë pragu dhe në qoftë se është më e vogël atëherë nyjet korresponduese konsiderohen si me qëllim të keq. Janë propozuar modele të ndryshme sigurie në MANET. Më poshtë jepen disa prej tyre.

Shafigh, A. S. Abdollahi, [35] propozuan metodën e kontrollit fuzzy logic për të përmirësuar performancën dhe besueshmërinë e protokolleve të rrugëzimit multicast në MANET. Krijohen grupe të vegjël dhe të fortë për uljen e konsumimit të burimeve dhe rritjen e stabilitetit. Një grup dërgimi përbëhet nga nyjet e forta/dobëta. Logjika fuzzy propozohet të përcaktojë nyjet e forta dhe të dobëta në rrjet. Në rrjet transmetohet periodikisht paketa *join query* për përditësimin e rrugëve në rrjet. Nyja e ndërmjetme mer një paketë *join query* jo të kopjuar, ruan ID e nyjes në tabelën e rrugëzimit dhe ri-transmeton paketën. Nyja që mer mesazhin *join query* duhet të konvertojë në vlera fuzzy parametrat si gjerësi e brezit, shpejtësia e nyjes dhe niveli i fuqisë. Vlerat e parametrit të nyjes paraardhëse përdoret për ta klasifikuar atë si: i ulët, mesatar, i lartë. Pas fuzzification, përdoret procesi i inference për të përcaktuar mundësinë e caching dhe transmetimin e *join query* në nyjet e tjera. Duke përdorur modelin fuzzy mund të marrin pjesë në transmetim vetëm linqet dhe nyjet që janë më robust ose kanë më shumë fuqi të disponueshme.

Morteza Romoozi and Hamideh Babaei, [36] propozuan një zgjerim të protokollit të zbulimit të përmbajtjes Gnutella në një sistem reputacioni. Sisteme të tillë e

konsiderojnë ç'organizimin e rrugëzimit si sjellje keqdashëse, ndërsa ky propozim shton si sjellje të re keqdashëse prishjen e politikës së sigurisë. Sistemi i propozuar përdor një sistem ekspert fuzzy për vlerësimin e nyjeve. Nëpërmjet këtij sistemi mund të importojmë disa rregulla sigurie të njohurive bazë dhe përdorimin e tyre për vlerësimin e nyjeve. Pra reputacioni i një nyje ndikohet nga politikat e sigurisë. Përveç kësaj një sistem fuzzy ndihmon sistemin për vlerësim më të saktë.

Arash Dana, Golnoosh Ghalavand, [37] propozon një algoritëm rrugëzimi të besueshëm bazuar në fuzzy logic. Këtu përcaktohen parametra si vlera e besueshmërisë dhe vlera e energjisë të cilat përdoren për gjetjen e një rruge të qëndrueshme nga burimi në destinacion. Gjatë zbulimit të rrugës, çdo nyje ruan vlerën e vet të besueshmërisë dhe kapacitetin e energjisë në paketën RREQ. Në destinacion, bazuar në vlerën e besueshmërisë vendoset cila rrugë do përzgjidhet. Rruga me vlerën më të madhe të besueshmërisë zgjidhet për rrugëzimin e paketave nga burimi në destinacion.

Partha Sarathi [38] propozoi përdorimin e AODV bazuar në fuzzy logic. Për besueshmërinë e nyjeve merren në konsideratë parametra të tillë si besueshmëria, energjia e mbetur, okupimi i buffer-it, shpejtësia e gjenerimit të paketave dhe shpejtësia e nyjes, më pas këto vlera dërgohen në rregullat fuzzy të bazuar në modulin e llogaritjes së besueshmërisë e cila jep vlerën korresponduese të besueshmërisë. Ky algoritëm është i aftë të mënjanojë nyjet egoiste. Meqenëse vetëm fqinjët e besueshëm përzgjidhen për dërgimin e paketave, konsumimi i energjisë ulet sepse nyjet nuk dërgojnë paketa në fqinjët e paautorizuar. Mungesa e nyjeve egoiste në fqinjët e zgjedhur në çdo hop siguron dërgim më të mirë të paketave dhe throughput më të mirë.

Nga studimi i literaturës dhe punimeve shkencore në fushën e sigurisë rezulton që më të shumtën janë propozuar protokolle të sigurtë për MANET si përmirësime të protokolleve egzistuese duke rritur efektivitetin e protokolleve egzistuese. Pra janë ndërtuar sisteme ose protokolle për një rrjet të caktuar (jo për çdo tip rrjeti MANET) ku rrugëzimi i paketave kryhet duke përdorur një protokoll rrugëzimi të caktuar.

Sistemet e bazuar në besueshmëri të diskutuar më lart për vlerësimin e besueshmërisë së rrjetit marrin në konsideratë parametra të tillë si lëvizshmëria e nyjes, energjia, shpejtësia e gjenerimit të paketave dhe shpejtësia e nyjes, mbi bazën e të cilëve përcaktojnë rrugën më të besueshme për transmetimit e paketave nga burimi në destinacion. Në të shumtën e punimeve të studiuar në këtë fushë nuk merret në konsideratë parametri i sigurisë së nyjeve.

Në sistemin tonë merret në konsideratë dhe siguria e nyjeve si parametër hyrje e cila rrit ndjeshëm besueshmërinë e nyjeve në cluster.

Gjithashtu modelet e propozuar në literaturë të diskutuar më sipër janë ndërtuar për një rrjet të caktuar MANET, ndërsa sistemet e propozuar në këtë punim janë ndërtuar për çdo lloj rrjeti MANET të përbërë nga nyje heterogjene dhe me karakteristika të caktuara (të cilat janë vlerësuar para se të futen në sistem nga algoritme të ndryshme) mbi bazën e të cilave bëhet vlerësimi i besueshmërisë. Për sistemet e propozuar në punim nuk ka rëndësi rrjeti, thjesht implementohet në çdo rrjet të ndarë në clustera duke përdorur një nga algoritmet e clustering në MANET.

Në këtë punim ne propozojmë dy sisteme të bazuar në fuzzy logic për përcaktimin dhe vlerësimin e besueshmërisë së nyjeve në cluster në MANET. Për të arritur qëllimin merren në konsideratë parametrat e hyrjes si numri i nyjeve në cluster, humbja e paketave, fuqia e shpenzuar dhe pastaj shtohet dhe siguria e nyjeve në cluster. Marrja në konsideratë e sigurisë së nyjeve rrit besueshmërinë e sistemit dhe përmirëson performancën e tij. Avantazhi i sistemeve të propozuar është që përjashton nga transmetimi i paketave nyjet të cilat konsiderohen si jo të besueshme nga sistemi.

Në këtë punim nuk propozohet një protokoll i ri, por propozohet një sistem i bazuar në fuzzy logic për përcaktimin dhe vlerësimin e besueshmërisë së nyjeve në cluster në MANET.

1.1.2 Sistemet e dedektimit të ndërhyrjeve (IDS)

Sistemi IDS është një metodë e integruar për dedektimin e sulmeve duke analizuar dhe monitoruar vazhdimisht aktivitetet e rrjetit.

Sistemi mund të jetë një host ose një server, një router ose gjithë rrjeti. Një sistem dedektimi mund të jetë një metodë përpunimi automatik të të dhënave e cila kontrollon dhe përdor aktivitetet në rrjet. Në MANET sistemet e dedektimit instalohen në çdo nyje. Egzistojnë dy tipe kryesore të skemave të dedektimit: watchdog dhe pathrater.

Watchdog funksionon si një njohje e ndërhyrjes për MANET e cila është përgjegjëse për identifikimin e sjelljes së keqe të nyjeve keqdashëse në sistem. Ajo zbulon sjelljen e keqe të nyjeve keqdashëse duke dëgjuar në mënyrë rastësore shpërndarjen në hop-in pasardhës. Në rastin e një nyje watchdog, ajo vëren që nyja pasuese neglizhon dërgimin e paketës në një kohëzgjatje të paracaktuar duke shkaktuar prishjen e numërimit nga nyjet, në këtë rast nyja watchdog e deklaron atë si mosbindje.

Strategjia Pathrater lejon nyjet të mbajnë larg nga përdorimi nyjet e pabindura në zgjedhje të ndryshme të ardhshme. Të dhënat e transmetuara aprovohen me mesazh. Sistemi Watchdog nuk është i aftë të vëzhgojë sjelljet infektuese në rastet e përplasjes së dykuptimësive.

Bayesian Watchdog vepron si sistem dedektimi të ndërhyrjeve i cili analizon dhe dëgjon trafikun e rrjetit për të dedektuar sjelljen e keqe. Pastaj ai llogarit vlerën e besueshmërisë për çdo fqinj. [31] Në qoftë se niveli i besueshmërisë është mbi pragun e caktuar atëherë nyja konsiderohet si nyje me qëllim të keq. Nga analiza e informacionit dytësor duke përdorur watchdog rritet performanca e sistemit që rezulton në uljen e mohimeve false dhe rritjen e shpejtësisë së dedektimit. Meqenëse rrugëzimi në MANET realizohet duke përdorur vlerën e besueshme atëherë përdoret sistemi i bazuar në besueshmëri. Në qoftë se vlera e besueshme është nën vlerën prag nyja korresponduese shënohet si me qëllim të keq dhe izolohet nga rrjeti duke rritur performancën e rrugëzimit në rrjet.

Kulbhushan Jagpreet Singh, paraqet një sistem dedektimi për MANET kundër sulmit blackhole duke përdorur logjikën Fuzzy. [31] Ky system dedekton blackhole në

rrjet dhe ky informacion kalohet në nyjet e tjera. Gjithashtu siguron një vlerësim të performancës për parametra të ndryshëm të rrjetit. Fuzzy logic është një zgjidhje e thjeshtë dhe efektive për dedektimin dhe izolimin e nyjes blackhole nga AODV në MANET. Logjika fuzzy përfshin një model të thjeshtë të bazuar në rregull në vend që të modelojë një sistem automatikisht. Për skenarë të ndryshëm provohet se sistemi i propozuar performon më mirë në gjithë parametrat si overhead-i i rrugëzimit, PDR dhe vonesa fund më fund.

Sergio Marti propozon klasifikimin e nyjeve bazuar në sjelljen tyre e matur në menyrë dinamike. [32] Përdoren dy teknikat watchdog dhe pathrater. Watchdog identifikon nyjet me qëllim të keq ndërsa pathrater ndihmon protokollet e rrugëzimit të shmangin këto nyje me sjellje të keqe në shqetësimin e rrjetit. Rezulton në rritje të throughput-it në rrjet.

Nidal Nasser [33] propozon një sistem dedektimi të ndërhyrjeve të quajtur Ex-watchdog për eliminimin e mangësive të watchdog. Ky sistem e zgjidh problemin e dedektimit të nyjes me sjellje të keqe e cila e ndan rrjetin duke njoftuar gabimisht nyjet e tjera si nyje me sjellje të keqe dhe jo veten. Ky funksionon duke dedektuar ndërhyrjen nga nyjet me qëllim të keq dhe njofton këtë informacion në përgjigjen e sistemit e cila është Path rater.

Varsha Himthani propozoi një teknikë për integrimin e informacionit egoist me filtrimin Bayesian. [34] Kjo rezulton në uljen e numrit të *false positives*. Kjo teknikë synon rritjen e dedektimit të nyjeve egoiste dhe me qëllim të keq në MANET. Duke përzier informacionin egoist me filtrimin Bayesian optimizon eficiencën e sistemit të dedektimit watchdog në MANET.

1.2 Motivimi

Qëllimi i teknologjisë pa tel është plotësimi i nevojës për shkëmbim të shpejtë, të besueshëm dhe të sigurtë të informacionit. Zhvillimi i teknologjisë MANET përpiqet t'i ofrojë përdoruesve në çdo kohë dhe kudo shërbimet në një rrjet pa tel pa infrastrukturë dhe heterogjen, bazuar në bashkëpunimin mes nyjeve të rrjetit.

Rritja e popullaritetit të MANET dhe përdorimi i tyre në mjedise të ndryshme ka nxitur skenarë të rinj ku siguria dhe besueshmëria e veprimeve të rrjetit është shumë e rëndësishme. Kjo shkaktohet nga rritja e rolit të rëndësishëm të MANET në shumë mjedise pa infrastrukturë dhe në aplikime si: emergjenca, rimëkëmbje nga fatkeqësi natyrore, institucione komerciale dhe akademike, biznes apo seminare ku përfshihen numër i madh njerëzish dhe ku pikat e aksesit janë të paarritshme apo mungojnë.

Meqenëse këto rrjeta vendosen në mjedis të hapur ku të gjitha nyjet bashkë veprojnë në dërgimin e paketave në rrjet, nyjet me qëllim të keq është e vështirë të dedektohen. Ndaj është e vështirë të ndërtohet një protokoll i sigurtë krahasuar me rrjetat me tel ose ato të bazuar në infrastrukturë.

Për shkak të mungesës së infrastrukturës, mungesës së pajisjeve të autorizimit dhe mjedisit të shpërndarë, mekanizmat tradicional të sigurisë nuk mund të aplikohen plotësisht në një rrjet MANET. Është e vështirë të bësh nyjet e lëvizshme të vendosin një lidhje të besuar afatgjatë me çdo nyje me të cilët ato janë lidhur përkohësisht.

Ky punim u motivua nga domosdoshmëria për krijimin e një rrjeti komunikimi të sigurtë të të dhënave në rrjetat MANET shumë të përdorshme në aplikime si emergjenca, fatkeqësi natyrore, biznes etj.

Lëvizshmëria e nyjeve si dhe mungesa e infrastrukturës në MANET e bën rrugëzimin një sfidë të rëndësishme. Rrugëzimi është procesi i zgjedhjes së një rruge për transmetimin e paketave nga nyja burim drejt destinacionit. Një nga problemet e rrugëzimit është mbingarkesa e rrjetit pasi kërkon informacin shtesë kontrolli për organizimin e nyjeve.

Një nga zgjidhjet e propozuar në literaturë për këtë problem është clustering.

Clustering rrit shkallëzueshmërinë e rrjetit, siguron një organizim hierarkik si dhe bën një shpërndarje efiçente të burimeve të rrjetit, që motivoi dhe përdorimin e clustering në MANET.

Gjithashtu aftësia e logjikës Fuzzy për të bërë modelimin gradual të karakteristikave të rrjetit duke marë parasysh informacionin e mbushur me pasiguri dhe

paqartësi, si dhe eksperiencën e ekspertëve motivoi përdorimin e logjikës Fuzzy për të vlerësuar dhe përmirësuar besueshmërinë e nyjeve cluster në MANET.
Logjika fuzzy është një metodë llogaritëse që mund të implementohet lehtë në cluster-a, dhe nuk kërkon shumë veprime llogaritëse.

1.3 Qëllimi dhe kontributi

Rrjetat e lëvizshme ad hoc janë rrjeta pa infrastrukturë, me shumë hope dhe dinamike. Këto rrjeta janë shumë të kërkuara për shkak të mungesës së infrastrukturës, efektivitetit në kosto dhe lehtësisë në instalim. Në këto rrjeta nuk kërkohet stacion bazë, këtu nyjet veprojnë si router për transmetimin e të dhënave te nyjet e tjera. Kështu rrugëzimi është një sfidë në këto rrjeta.
Për t'a bërë më efektiv rrugëzimin në MANET si dhe për të ulur mbingarkesën e rrjetit përdoret teknika clustering e cila është një teknikë e rëndësishme për organizimin hierarkik në rrjetat e lëvizshme ad hoc. Clustering ndihmon në uljen e kompleksitetit, në menaxhimin e informacionit rreth nyjeve të lëvizshme dhe thjeshton procesin e rrugëzimit.

Duke njohur karakteristikat e algoritmeve të ndryshëm clustering si dhe avantazhet e secilit mund të arrihet të përftohet një performancë e mirë e rrjetit. Për të përcaktuar dhe përmirësuar besueshmërinë e nyjeve cluster në MANET, propozohet përdorimi i kontrollerit logjik fuzzy si më e përshtatshme për këtë sistem. Zgjedhja e nyjeve në cluster më të besueshme përmirëson ndjeshëm performancën e gjithë sistemit.

Qëllimi i punimit është propozimi i sistemeve të bazuar në logjikën Fuzzy për përcaktimin e besueshmërisë së nyjeve cluster në MANET dhe implementimi i sistemeve të propozuar për vlerësimin e besueshmërisë së nyjeve.
Duke u bazuar në kontrollerin logjik fuzzy përcaktohet për çdo nyje në cluster nëse është e besueshme për të marrë pjesë në transmetimin e paketave. Nëse nuk është e besueshme nyja përjashtohet nga procesi i transmetimit të paketave (largohet nga cluster-i).
Gjithashtu ky punim ka si qëllim përmirësimin e besueshmërisë së nyjeve cluster, si dhe vlerësimin dhe krahasimin e performancës së sistemeve të propozuar.

Kontributi ynë në këtë punim qëndron në propozimin e një sistemi për vlerësimin e besueshmërisë së nyjeve cluster duke përdorur logjikën fuzzy.

Kontributet në një këndvështrim tjetër janë:

- Propozimi i një sistemi për përcaktimin nëse një nyje duhet të mbetet në cluster ose jo bazuar në kushtet që duhet të plotësojë.
- Përmirësimi i sistemit të parë të propozuar duke shtuar si parametër në hyrje dhe sigurinë e nyjeve në cluster.
- Implementimi dhe vlerësimi i sistemeve të propozuar.

1.4 Struktura e disertacionit

Punimi është organizuar si më poshtë:

Kapitulli 1 jep një tablo të përgjithshme të disertacionit duke u fokusuar në analizën e punimeve kërkimore – shkencore të viteve të fundit në fushën e sigurisë në rrjetat MANET. Bazuar tek motivimi i punimit parashtrohen qëllimi dhe objektivat për t'u përmbushur.

Kapitulli 2 paraqet një përshkrim të përgjithshëm të rrjetave MANET, duke u ndalur te karakteristikat e këtyre rrjetave. Paraqet dhe një analizë të protokolleve të rrugëzimit si dhe të algoritmeve të bazuar në cluster në MANET.

Kapitulli 3 trajton sigurinë në MANET. Paraqiten aspekte të ndryshme të sigurisë si dhe mekanizmat e sigurië. Paraqitet dhe një analizë e sulmeve të ndryshëm në këto rrjeta sipas shtresave të MANET. Gjithashtu janë analizuar disa protokolle të sigurtë në MANET.

Kapitulli 4 paraqet logjikën Fuzzy. Paraqitet një analizë e plotë e sistemeve fuzzy logic duke u ndalur tek kontrolli fuzzy logic, fuzzification, funksionet e anëtarësimit, funksionimi i sistemit inference fuzzy, defuzzification, marrja e vendimeve.

Kapitulli 5 trajton analizën e sistemeve të propozuar. Jepen rezultatet eksperimentale të kryera për të dy sistemet e propozuar dhe analiza e rezultateve.

Disertacioni mbyllet me përfundime dhe objektiva në të ardhmen.

KAPITULLI 2

RRJETAT MOBILE AD-HOC (MANET)

2.1 Hyrje

Komunikimi pa tel është çelësi për disponueshmërinë e rrjetit kudo dhe në çdo kohë. [1] Sistemet e sotëm të komunikimit pa tel zakonisht varen nga infrastruktura të para-përcaktuara të komunikimit. Rrjetat MANET lejojnë komunikimin ku nuk ka infrastrukturë të tillë të disponueshme. Ato janë të vetë organizuara dhe vetë konfiguruara. Nyjet veprojnë si pika fundore dhe rutera komunikimi. Komunikimi multi-hop është i mundur nëpërmjet bashkë veprimit të nyjeve dhe protokolleve të rrugëzimit ad hoc. Rrjetat MANET gjejnë aplikim në sallat e konferencave, në rrjetat e operacioneve ushtarake si dhe në ndihmën ndaj fatkeqësive natyrore. Këto rrjeta pritet të luajnë një rol të rendësishëm në sistemet e komunikimit në të ardhmen në raste fatkeqësish natyrore ku nuk mund të mbështetet në një infrastrukturë fikse. Gjithashtu MANET mund të përdoren për zgjerimin e zonës së mbulimit ose zvogëlimin e ngarkesës në stacionet bazë dhe pikat e aksesit në sistemet e komunikimit të bazuar në infrastrukturë. Përdoruesit pritet që të parashikojnë të njëjtin grup shërbimesh që ato përdorin në një rrjet me tel të përdoren dhe në MANET. Për të arritur këto objektiva, komunikimi pa tel multi-hop përballet me sfida dhe kufizime të tjera në krahasim me rrjetet me tel. Këto kufizime mund të jenë konsumi i energjisë, caktimi i frekuencave për rrugëzimin dhe siguria. Shembull i një rrjeti MANET jepet në figurën 2.1.

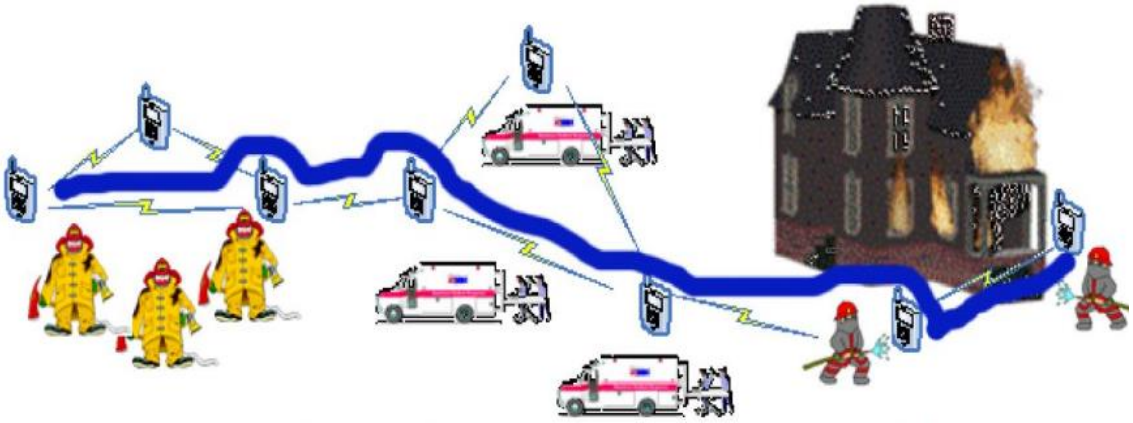


Figura 2.1. Një rrjet Mobile Ad hoc

Rrjeti me sensorë është një kategori e veçantë e rrjetave mobile ad hoc që konsiston në sensorë të ndryshëm të lidhur pa ndonjë infrastrukturë fikse. [1] Diferenca ndërmjet rrjetave me sensorë dhe rrjetave të lëvizshëm ad hoc të zakonshëm është që nyjet sensorë nuk janë domosdoshmërisht të lëvizshëm. Gjithashtu numri i nyjeve është më i madh se rrjetat e zakonshëm ad hoc. Një rrjet me sensorë wireless konsiston në vendosjen e nyjeve sensorë në një mjedis gjeografik për monitorimin e fenomeneve fizikë si temperatura, lagështia, lëkundjet, ngjarje sizmike etj. Zakonisht një nyje sensor është një pajisje e vogël që përfshin tre komponentë bazë: një nënsistem të ndjeshëm për mbledhjen e të dhënave nga mjedisi fizik përreth, një nënsistem përpunimi për ruajtjen dhe përpunimin e të dhënave lokale, dhe një nënsistem komunikimi pa tel për transmetimin e të dhënave. Përveç kësaj, dhe një burim fuqie për furnizimin me energjinë e nevojshme për pajisjen për të kryer detyrën e programimit. Ky burim energjie konsiston në një bateri me energji të kufizuar. Eshtë pothuajse e pamundur ose e papërshtatshme rimbushja e baterisë sepse nyjet mund të vendosen në mjedise jopraktikë dhe jo të favorshëm. Nga ana tjetër rrjetat me sensorë duhet të kenë një jetëgjatësi të mjaftueshme për të përmbushur kërkesat e aplikimeve.

2.2 Karakteristikat e rrjetave MANET

Një rrjet MANET përbëhet nga nyjet që veprojnë si host dhe router dhe që mund të lëvizin lirisht pa asnjë lloj arbitrariteti. Nyjet mund të ndodhen në aviona, anije, makina, ose në pajisje të vogla dhe mund të jenë hoste të shumta për një router. [1], [5] MANET është një sistem autonom i nyjeve të lëvizshme. Sistemi mund të operojë i izoluar ose të ketë porta dhe ndërfaqe drejt një rrjeti tjetër fiks dhe kjo mënyrë operimi quhet rrjet "stub " i lidhur me një nënrrjet fiks. Rrjetat "stub " mbartin trafikun e gjeneruar/destinuar për nyjet e brendshme por nuk lejojnë kalimin e trafikut të jashtëm përmes rrjetit në fjalë.

Nyjet MANET janë të pajisura me transmetues dhe marrës pa tel duke përdorur antenat që mund të jenë broadcast, pikë më pikë ose kombinime të tyre. Në një moment të caktuar kohe në varësi të pozicionit të nyjeve dhe karakteristikave të mbulimit të antenave transmetuese dhe marrëse, niveleve të fuqisë së transmetimit dhe niveleve të interferencës midis kanaleve, egziston rrjeti ad-hoc midis nyjeve. Kjo topologji ad-hoc mund të ndryshojë në kohë si rezultat i lëvizjes së nyjeve dhe rregullimit të parametrave të tyre të transmetimit dhe marrjes. [4]

Rrjetat MANET kanë disa karakteristika:

- Topologji dinamike: Nyjet mund të lëvizin lirisht pa kufizime arbitrare dhe rrjedhimisht topologjia multihop e rrjetit mund të ndryshojë shpejt dhe rastësisht në kohë të paparashikuara dhe mund të përbëhet nga linja një dhe dy drejtimëshe.
- Kufizimet e Gjerësisë së brezit dhe kapacitetet e ndryshme të linjave: Linjat pa tel do vazhdojnë të kenë kapacitete më të ulëta se pjesa tjetër e linjave të lidhura. Throughputi i linjave pa tel është më e vogël se shpejtësia maksimale e transmetimit radio, kjo si rezultat i ndikimit të efekteve të shuarjes, interferencës, aksesit të shumëfishtë, zhurmave etj. Arsyeja kryesore e aftësisë së ulët për të ndryshuar kapacitetin e linjave lidhet me mbipopullimin e rrjetit.
- Operimi me Energji të kufizuar: Disa ose të gjitha nyjet në rrjetin MANET mbështeten tek bateritë si burimin e tyre të energjisë. Për këto nyje kriteri më i rëndësishëm për optimizimin e rrjetit është kursimi i energjisë.

- Siguria fizike e kufizuar: Rrjetat e lëvizshëm pa tel janë më shumë objekt i kërcënimeve të sigurisë fizike sesa rrjetat kabllore fikse. Duhet konsideruar mundësia e madhe e sulmeve si humbja e shërbimit, dëgjimi dhe vjedhja e informacionit. Teknikat egzistuese të sigurisë së linjave aplikohen brenda rrjetave pa tel për të reduktuar kërcënimet e sigurisë. Si përfitim, natyra e decentralizuar e kontrollit në rrjetat MANET siguron fortësi më të madhe kundrejt pikave të dështimit.

Disa rrjeta MANET janë të mëdha në përmasa (rrjetat ushtarake ose në metro) dhe përbëhen nga mijëra nyje dhe rrjedhimisht lind nevoja për shkallëzueshmëri të madhe.

2.3 Rrugëzimi në MANET

Rrugëzimi në rrjetat ad-hoc është procesi i përzgjedhjes së rrugëve në një rrjet me të cilin një paketë udhëton nga një burim në një destinacion në kohën e duhur, kështu çdo nyje vepron si një router po ashtu dhe si një nyje fundore për të transmetuar ose për të marrë paketa në rrjet. [10] Rrugëzimi është një detyrë e frikshme në MANET për shkak të karakteristikave të rrjetit që lidhen me lëvizshmërinë e nyjeve, vetë organizimin, komunikimin hop to hop dhe burimet e kufizuara.[15] Janë propozuar protokolle të ndyshme në literaturë për rrugëzimin në rrjetat e lëvizshëm ad hoc që janë shumë eficient. Në thelb, të gjithë protokollet e rrugëzimit përpiqen të gjejnë një rrugë optimale nga burimi në destinacion, duke pranuar që të gjitha nyjet në rrjet janë të besueshme dhe bashkëpunuese. Një nga aspektet më interesante të këtyre kërkimeve konsiston në atë që një nyje në rrjet duhet të mbajë gjurmët e rrugëve për të gjitha destinacionet e mundshme, apo vetëm gjurmët e atyre destinacioneve me interes të menjëhershëm, sepse një rrugë e themeluar nga një burim nuk mund të ekzistojë pas një intervali të shkurtër kohe. Në varësi se si nyjet vendosin dhe mirëmbajnë një rrugë drejt destinacionit të kërkuar, protokollet e rrugëzimit për rrjetat ad hoc ndahen në proaktivë, reaktivë dhe hibridë siç paraqiten në figurën 2.2.

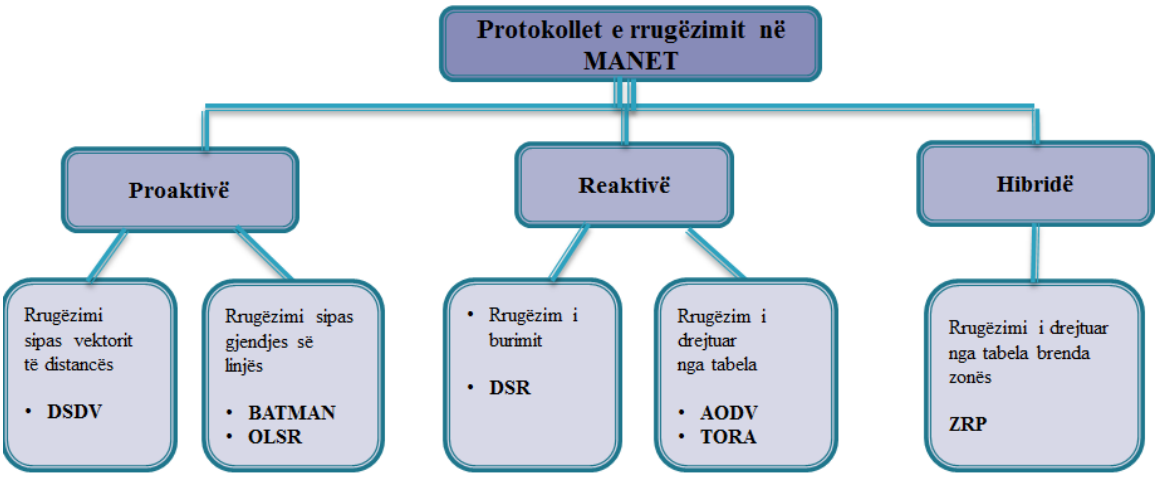


Figura 2.2. Protokollet e rrugëzimit në MANET

2.3.1 Protokollet Proaktivë në rrjetat MANET

Protokollet proaktivë janë protokolle bazuar në tabela, ku çdo nyje përpiqet të mbajë të rifreskuar informacionit e rrugëzimit për çdo nyje në rrjet duke mbajtur një ose më shumë tabela. [2] Informacioni i rrugëzimit ruhet dhe mbahet para se të fillojë transmetimi. Kjo ka avantazhin që ka një vonesë fillestare minimale meqenëse rruga e dëshiruar është venddosur tashmë. Megjithatë, protokollet proaktive shkaktojnë trafik të konsiderueshëm sinjalizimi dhe problem në konsumin e energjisë, si dhe mbingarkesë të lartë për shkak të mirëmbajtjes së rrugës dhe të rifreskimeve të shpeshta të rrugës.

Protokollet proaktive të rrugëzimit ndahen në dy nënkategori:

Kategoria e Rrugëzimit sipas Gjendjes së Linjës- Këtu nyjet përdorin periodikisht mesazhet “Hello” dhe “Topology Control (TC)” për të zbuluar dhe shpërndarë informacionin e njohur mbi lidhjen e nyjes. Ky informacion përshkruan gjendjen e lidhjeve që lidhin nyjet e ndryshme. Çdo nyje burim shpërndan periodikisht një mesazh “HELLO”. Çdo nyje fqinje një hop larg nyjes burim i përgjigjet asaj që janë fqinje. Nyja dërguese pastaj gjeneron dhe një mesazh TC, i cili rrjedh nëpër rrjet. Mesazhet TC informojnë nyjet e tjera rreth lidhjes ndërmjet nyjes burim dhe fqinjëve të saj të afërt. Ato lejojnë çdo nyje të ndërtojnë një hartë rrjeti dhe të llogarisin hopin pasardhës, ose të

gjithë rrugën, drejt gjithë destinacioneve. Shembuj të kësaj kategorie protokollesh është protokolli OLSR (Rrugëzimi sipas gjendjes së linjës i optimizuar), BATMAN (Model më i mirë në rrjetat MANET) etj.

2.3.1.1 Rrugëzimi sipas gjendjes së linjës i optimizuar (OLSR)

Protokolli OLSR është vazhdimësi i rrugëzimit tradicional i gjendjes së linkut, i modifikuar për të siguruar operimin në rrjetet ad hoc. [9] Karakteristika e OLSR është përdorimi i multipoint relays (MPR) për zvogëlimin e mbingarkesës së rrjedhjeve të rrjetit dhe numrin e përditësimeve të gjendjes së linkut. Çdo nyje llogarit MPR e saj nga grupi i fqinjëve të saj.[15] MPR përzgjidhet e tillë që kur një nyje shpërndan një mesazh, ritransmetimi i këtij mesazhi nga MPR do të sigurojë që mesazhi është marrë nga çdo fqinjë dy hope larg saj. Kështu, kur një nyje shpërndan një mesazh, vetëm këto fqinjë në MPR e saj rishpërndajnë mesazhin. Fqinjët e tjerë që nuk janë në grupin e MPR e përpunojnë mesazhin por nuk e rishpërndajnë atë. Më tej kur shkëmbehet informacioni i gjendjes së linkut, një nyje vetëm rendit lidhjet e saj me fqinjët që e kanë përzgjedhur atë si MPR. Meqenëse OLSR është protokoll proaktiv, çdo nyje mban një rrugë drejt çdo nyje tjetër në rrjet. Kur nyja merr mesazhet TC nga nyjet e tjera të rrjetit, ajo mund të krijojë ose modifikojë hyrjet e rrugëzimit në çdo nyje në rrjet duke përdorur algoritme rrugëzimi me rrugën më të shkurtër, të tillë si algoritmi Dijkstra.

Kategoria e Vektorit të Distancës: Këtu nyjet ndërtojnë dhe shpërndajnë periodikisht tabelat e rrugëzimit të cilat përmbajnë destinacionet e arritshme dhe numrin e hopeve për të arritur ato, ose dhe disa metrika të tjera. Nyjet vazhdimisht rifreskojnë tabelat e tyre të rrugëzimit bazuar në tabelat e marra nga fqinjët e tyre. Këtu mund të përmendim protokollin DSDV (Vektori distancë hap pas hapi).

2.3.1.2 Vektori distancë hap pas hapi (DSDV)

Eshtë një protokoll rrugëzimi i nisur nga tabela që bazohet në një version të algoritmit Bellman Ford. DSDV kërkon që çdo nyje të rifreskojë rrugëzimin e transmetimit periodikisht. Një kufizim i DSDV është që ai siguron vetëm një rrugë për

burimin/destinacionin. [13] Avantazhi i DSDV ndaj protokolleve tradicional të vektorit të distanës është që ky është i pavarur nga ciklet. Çdo nyje DSDV mban një tabelë rrugëzimi ku rendit hapin pasardhës për çdo desinacion të arritshëm. Çdo hyrje tabele ka një numër sekuence që rritet sa here që një nyje dërgon mesazhin e rifreskuar. Tabelat e rrugëzimit rifreskohen periodikisht kur ndryshon topologjia e rrjetit dhe përhapen nëpër rrjet për të mbajtur informacion të qëndrueshëm mbi rrjetin. Çdo nyje DSDV mban dy tabela rrugëzimi: një për paketat e dërgimit dhe një për njoftimin e paketave të rrugëzimit rritëse. Informacioni i rrugëzimit i dërguar periodikisht nga një nyje përmban një numër sekuence të ri, adresën e destinacionit, numrin e hopeve të nyjes destinacion dhe numrin e sekuencës të destinacionit. Kur ndryshon topologjia e rrjetit, një nyje dedektuese dërgon një paketë rifreskimi në nyjet fqinje të saj.

2.3.2 Protokollet reaktivë

Në kushtet e fuqisë së limituar dhe gjeresisë së brezit, do të ishte mirë të minimizohej trafiku i kontrollit të rrugëzimit kur nuk ka të dhëna për tu rrugëzuar. Rrugëzimi proaktiv nuk është i përshtatshëm në këtë rast. Ky është motivimi kryesor i rrugëzimit reaktiv, i quajtur gjithashtu dhe sipas kërkesës (on-demand). Këto protokolle nuk mbajnë rrugë, por i ndërtojnë ato on-demand kur kërkohet komunikimi për në një destinacion të caktuar.[2], [3] Këtu mund të përmendim AODV(Vektori distancë sipas kërkesës), DSR (Rrugëzimi i burimeve dinamike). Dhe për këtë klasë protokollesh kemi ndarjen në dy nënkategori kryesore :

Rrugëzimi iniciohet nga burimi – në këtë rast protokolli kryesor përfaqësues është protokolli DSR (Rrugëzimi i burimit dinamik). Një protokoll i ngjashëm me AODV pasi inicion kërkimin e një rruge vetëm kur kërkohet por ndryshe nga AODV-ja përdor rrugëzimin nga burimi në vend që të bazohet në tabelat e rrugëzimit të secilës nyje të ndërmjetme.

2.3.2.1 Vektori distancë sipas kërkesës (AODV)

Algoritmi i rrugëzimit vektori distancë sipas kërkesës është një protokoll rrugëzimi i ndërtuar për rrjetet e lëvizshëm ad hoc. [8] AODV mundëson rrugëzimin unicast dhe multicast. Eshtë një algoritëm sipas kërkesës, që do të thotë se ndërton rrugë ndërmjet nyjeve vetëm kur kërkohet nga nyjet burim. AODV përdor numrat e sekuencës për të siguruar origjinalitetin e rrugës. Nuk vuan nga formimi i cikleve, është i vetë startuar dhe i shkallëzueshëm për numër të madh nyjesh të lëvizshme. Ky protokoll ndërton rrugë duke përdorur ciklin pyetës kërkesë rruge (RREQ)/përgjigje rruge (RREP). Kur një nyje burim dëshiron një rrugë për në destinacion për të cilin nuk ka një rrugë ta gatshme, ai shpërndan një paketë kërkesë rruge (RREQ) përmes rrjetit. Përveç adresës IP të nyjes burim, numrit sekuencial aktual dhe ID së transmetimit, RREQ përmban gjithashtu dhe numrin sekuencial më të fundit për destinacionin për të cilin nyja burim është e vetdijshme. Nyja që mer RREQ mund të dërgojë një RREP nqs ajo është destinacioni ose nqs ka një rrugë për në destinacion me numrin e sekuencës korresponduese më të madh ose të njëjtë me atë të RREQ. Në këtë rast, ai dërgon mbrapsht një RREP për në burim. Pasi burimi merr RREP, ai mund të fillojë dërgimin e të dhënave për në destinacion. Avantazhi i AODV është që ai përpiqet të minimizojë numrin e transmetimeve të kërkuara. Ai krijon rrugët sipas kërkesës, që presupozon të mbajë listën e plotë të rrugëve për çdo destinacion.

2.3.2.2 Rrugëzimi i burimeve dinamike (DSR)

Eshtë një protokoll rrugëzimi sipas kërkesës. Në DSR rrjeti është plotësisht i vetorganizuar dhe vetkonfiguruar, pa patur nevojën për ndonjë infrastrukturë rrjeti egzistuese. Përbëhet nga dy faza: zbulimi i rrugës dhe mirëmbajtja e rrugës që i lejon nyjet të zbulojnë dhe mirëmbajnë rrugët e burimit drejt destinacioneve arbitrare në rrjetin ad hoc. DSR mban një memorie rruge e cila mban gjurmët e të gjitha rrugëve. Kur një nyje duhet të dërgojë një paketë për në destinacion ajo fillimisht kontrollon memorien e

saj nqs ajo di një rrugë për në destinacion.[10] Nqs rruga për në destinacion nuk është në dispozicion në memorien e rrugës atëhere fillon mekanizmi i zbulimit të rrugës. Zbulimi i rrugës lejon një host të rrjetit ad hoc të zbulojë në mënyrë dinamike një rrugë për tek një host tjetër në rrjet. Nqs paketa kërkesë RREQ arrin destinacionin ai kthen mbrapsht përgjigjen e rrugës, ose nqs RREQ arrin një nyje të ndërmjetme që ka një rrugë aktive për në destinacion në cachen e saj. Procedura e mirëmbajtjes së rrugës mban kontrollin mbi funksionimin e rrugëve dhe informon dërguesin për ndonjë gabim në rrugëzim. Ky protokoll vepron tërësisht sipas kërkesës, duke lejuar overhead-in e paketës së rrugëzimit të DSR të shkallëzohet automatikisht vetëm tek ato që duhet të reagojnë ndaj ndryshimeve në rrugët aktualisht në përdorim.

Protokollet e drejtuara nga Tabelat – ku bëjnë pjesë një nr i madh protokollesh ku më të njohurit janë AODV dhe TORA. TORA është një protokoll rrugëzimi gjeopozicional dhe është shumë më pak i përdorur krahasuar me protokollin AODV.

2.3.2.3 Algoritmi i rrugëzimit përkohësisht i rregulluar-TORA

TORA është ndërtuar për të zbuluar rrugët sipas kërkesës, të sigurojë rrugë të shumëfishta drejt destinacionit, të krijojë shpejt rrugët, dhe të minimizojë mbingarkesën e komunikimit. Ky protokoll përdor gjatësinë si parametër arbitrar për të përcaktuar drejtimin e lidhjes ndërmjet dy nyjeve për një destinacion të dhënë. Rrjedhimisht, egzistojnë rrugë të shumta për një destinacion të caktuar por asnjëra prej tyre nuk është domosdosmerisht më e shkurtra. [7] Për të filluar një rrugë, nyja shpërndan një paketë Query tek fqinjët e saj. Kjo Query rishpërndahet nëpër rrjet derisa arrin destinacionin ose një nyje të ndërmjetme që ka një rrugë për në destinacion. Marrësi i paketës Query pastaj shpërndan paketën Update e cila rendit gjatësinë e saj në lidhje me destinacionin. Nqs nyja nuk ka fqinjë me gjatësi të fundme në lidhje me destinacionin, atëhere nyja do të përpiqet të zbulojë një rrugë të re. Kur një nyje dedekton një ndarje rrjeti, ajo gjeneron një paketë Clear që rezulton në rifillimin e rrugëzimit në rrjetin ad hoc. Një nga përfitimet e TORA është se suporton rrugë të shumta nga burimi drejt destinacionit. Kështu, dështimi apo largimi i ndonjë nyje zgjidhet menjëherë pa ndërhyrjen e burimit për

kalimin në një rrugë alternative. Një kufizim i këtij protokolli është që varet nga sinkronizimi ndërmjet nyjeve në rrjet.

2.3.3 Protokollet Hibridë

Këto protokolle kombinojnë rrugëzimin lokal proaktiv dhe rrugëzimin global reaktiv për të rritur eficiencën dhe shkallëzueshmërinë. Megjithatë, edhe një kombinim i të dy strategjive ende ka nevojë të mbajë të paktën ato shtigjet e rrjetit që janë aktualisht në përdorim, duke kufizuar sasinë e ndryshimeve topologjike që mund të tolerohen brenda një intervali të caktuar kohe. Këtu përfshihet protokolli ZRP.

2.3.3.1 Protokolli i rrugëtimit në zona (ZRP)

ZRP është një hibrid i protokollit reaktiv dhe proaktiv. Ai ndan rrjetin në disa zona rrugëzimi dhe specifikon dy protokolle të veçuar plotësisht që operojnë brenda dhe ndërmjet zonave të rrugëzimeve. [3] ZRP u ndërtua për zvogëlimin e mbingarkesës së protokolleve. ZRP konsiston në komponente që funksionojnë të pavarur për të dhënë rezultat efficient si IARP (protokolli i rrugëzimit intrazonë), IERP (Protokolli i rrugëzimit interzonë).

Protokolli i rrugëzimit intrazone (IARP) operon brenda zonës së rrugëzimit, mëson distancën më të vogël dhe rrugëzon tek të gjitha nyjet brenda zonës. Protokolli nuk është i përcaktuar dhe mund të përfshijë një numër të protokollit proaktiv, siç është “vektori i distancës” ose “rrugëzimi i gjendjes së lidhjes”. Një ndryshim në topologji nënkupton se informacioni i rifreskuar shpërndahet vetëm brenda zonave të rrugëzimeve të prekura dhe që nuk mund të prekin të gjithë rrjetin.

Protokolli i rrugëzimit Interzone (IERP) është reaktiv dhe përdoret për zbulimin e rrugëve ndërmjet zonave të rrugëzimeve të ndryshme. Kjo është e dobishme nëse nyja e destinacionit nuk vendoset brenda zonës së rrugëzimit. Atëhere protokolli transmeton një RREQ për të gjitha nyjet kufitare brenda zonës së rrugëzimit, e cila në kthim dërgon kërkesën, nëse nyja e destinacionit nuk u gjend brenda zonës së tyre të rrugëzimit.

Kjo procedurë përsëritet deri sa nyja e kërkuar gjendet dhe një përgjigje rrugëzimi kthehet tek burimi që tregoi rrugëzimin. Meqënëse ZRP është një protokoll hibrid ndërmjet skemave proaktive dhe reaktive, ky protokoll përdor avantazhe nga të dyja.

2.3.4 Clustering në MANET

Një nga problemet kryesore të skemave të rrugëzimit në rrjetat MANET është mbingarkesa e informacionit të kontrollit i kërkuar për organizimin autonom sipas lëvizshmërisë së nyjes. [24] Skema e rrugëzimit bazuar në cluster siguron një zgjidhje të këtij problemi duke i organizuar nyjet në cluster-a për të ulur mbingarkesën. Në sistemet e shpërndara komplekse, përdorimi i teknikës clustering rezulton në thjeshtimin e adresimit dhe menaxhimit të nyjeve dhe gjithashtu jep performancë më të mirë. Prandaj përdorimi i organizimit hierarkik sjell përfitime në menaxhimin e sistemeve kompleksë dhe në shkallëzueshmërinë e veprimeve.

Clustering është një teknikë e ndarjes së rrjetit në njësi të vogla dhe të vet-menaxhueshme që quhen cluster-a. [52] Çdo cluster ka një nyje të veçantë të zgjedhur si CH bazuar në një metrikë specifike ose kombinim i metrikave të tilla si identiteti, niveli, lëvizshmëria, ngarkesa, densiteti etj. CH luan rolin e koordinatorit brenda cluster-it të tij. Çdo CH vepron si një stacion bazë i përkohshëm brenda cluster-it dhe komunikon me CH-të e tjerë. Një cluster përbëhet nga një cluster head, nyja gateway dhe nyja e zakonshme ose anëtare. Shembull i clustering në MANET paraqitet në figurën 2.3.

Cluster head (CH): është koordinatori i cluster-it.

Gateway: është një nyje e zakonshme nërmjet dy ose më shumë cluster-ve.

Nyja anëtare: është një nyje që nuk është as CH dhe as gateway.

Çdo nyje i përket ekskluzivisht një cluster-i pavarësisht fqinjëve të saj që mund të vendosen në cluster-a të ndryshëm. Në figurën më poshtë jepet skema e clustering në MANET.

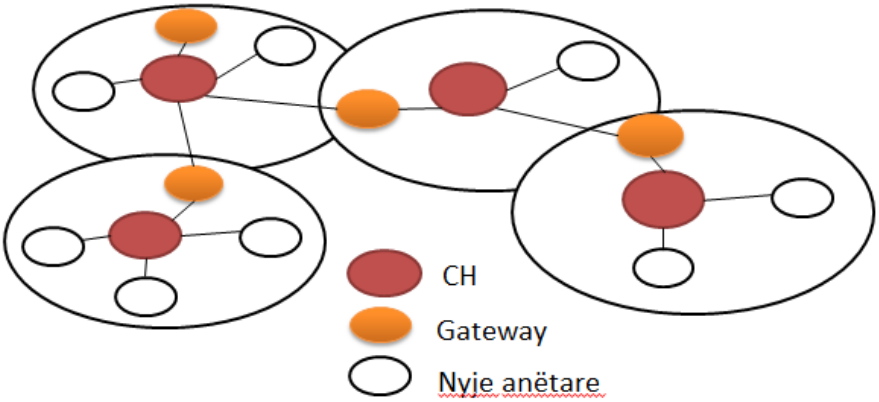


Figura 2.3. Clustering në MANET

2.3.5 Protokollet e rrugëzimit të bazuar në Cluster

Formimi i cluster-it bëhet duke përdorur dy mekanizma: Clustering i bazuar në identifikues, një nyje vet zgjidhet si cluster head nqs ka ID më të vogël/madhe në fqinjësinë e saj. Clustering i bazuar në lidhshmëri, nyja që ka më shumë nyje fqinjë zgjidhet si cluster head. Më poshtë jepen disa algoritme të ndryshëm clustering.

2.3.5.1 Algoritmi clustering d-Hop i bazuar në lëvizshmëri (MobDHop)

Ky algoritëm formon në mënyrë dinamike cluster-a të qëndrueshëm të cilët mund të shërbejnë si bazë e arkitekturës së rrugëzimit. Fillimisht MobDHop formon cluster-a me 2 hop jo të mbivendosur si algoritmet e tjerë clustering. [26] Më pas, këto clustera fillojnë një proces bashkimi ndërmjet nyjeve të tjera në qoftë se ato mund të dëgjojnë një tjetër përmes nyjeve gateway. Procesi i bashkimit do të jetë i sukseshmëm vetëm nëse cluster-i i ri i formuar arrin nivelin e kërkuar të stabilitetit. Siç vihet re, shumica e algoritmeve egzistues clustering formojnë clustera 2 hop që nuk mund të jenë shumë të përdorshëm në rrjeta të mëdha. Kështu, MobDhop është ndërtuar për të formuar clustera d hop që janë më fleksibël në diametrin e cluster-it. Diametri i cluster-ve është i përshtatshëm me modelin e lëvizshmërisë së nyjeve të rrjetit. Ky algoritëm është i

thjeshtë dhe shkakton mbingarkesë sa më të ulët. Shkëmbimi i informacionit gjatë formimit të cluster-ve dhe ndryshimet e CH mbahen në minimum.

2.3.5.2 Algoritmi clustering i bazuar në parashikimin e lëvizshmërisë (MPBC)

Ky algoritëm është ndërtuar për lëvizjen rastësore dhe të pavarur të nyjeve. Gjatë fazes së clustering, të gjitha nyjet transmetojnë periodikisht paketat Hello për të ndërtuar listat e fqinjëve të tyre.[30] Çdo nyje vlerëson shpejtësitë relative mesatare të saj në lidhje me të fqinjëve bazuar në shkëmbimet e paketave Hello. Nyjet me lëvizshmërinë relative më të ulët përzgjidhen si CH. Gjatë fazës së mirëmbajtjes së clusterit përdoret metoda e bazuar në parashikim për të zgjidhur problemet e shkaktuara nga lëvizjet relative të nyjes, duke përfshirë rastet kur një nyje lëviz jashtë zonës së mbulimit të CH të saj, dhe kur dy CH lëvizin brenda zonës së njëri tjetrit, njëri kërkohet të heqë dorë nga roli si CH. Ky algoritëm siguron jetëgjatësi të madhe të CH, që rezulton në cluster-a të qëndrueshëm.

2.3.5.3 Algoritmi me CH me afërsi ndërmjet tyre 3 hop (3-hBAC)

Ky algoritëm përfshin një status të ri të nyjes që quhet cluster guest i cili krijon një strukturë cluster-ash me 1 hop, jo të mbivendosur me tre hope ndërmjet CH fqinje. Nyja cluster guest është një nyje e lëvizshme e cila nuk mund të lidhet direkt me ndonjë CH por mund të aksesojë disa cluster-a me ndihmën e një anëtari të cluster-it.[25] [29] Nyja e lëvizshme me nivelin më të lartë zgjidhet si CH i parë. Nyja e lëvizshme që nuk është pranuar si CH, deklarohet si një CH i ri kur ka nivelin më të lartë në fqinjësinë e saj. Fqinjët me distancë 1 hop bashkohen si nyje anëtare. Nyjet fqinje të këtyre nyjeve anëtare që nuk mund t'i bashkohen direkt një cluster-i deklarohen si cluster guest. Për mirëmbajtjen e cluster-it, algoritmi mban CH me afërsi të paktën 2 hope. Ky algoritëm ul numrin e CH dhe eleminon cluster-at e vegjël të panevojshëm.

2.3.5.4 Algoritmi clustering me ID lidhjeje k-hope (KCONID)

Algoritmi KCONID kombinon dy algoritme clustering: ID më të ulët dhe metodën e nivelit më të lartë. Për zgjedhjen e CH-ve, si kriter i parë konsiderohet lidhja

dhe si kriter i dytë ID më e ulët.[25], [27] Për qëllimin e lidhjes duke përdorur vetëm lidhjen e nyjes si kriter shkakton lidhje të ndryshme ndërmjet nyjeve dhe nga ana tjetër duke përdorur vetëm kriterin e ID më të ulët gjenerohen më shumë cluster-a se sa duhen. Qëllimi kryesor është minimizimi i numrit të cluster-ave të formuar në rrjet. Culster-at në modelin KCONID formohen nga një CH dhe gjithë nyjet që janë në një largësi jo më shumë se k-hope nga CH. Ndryshe nga metoda e nivelit më të lartë, ku niveli i nyjes është vetëm madhësia e lidhjes për cluster me 1 hop, ky algoritëm formon një lidhje e cila përgjithësohet për një fqinjësi me k hope. Një nyje përzgjidhet si CH në qoftë se ka lidhje më të lartë. Në rastin e lidhjes uniforme, një nyje ka prioritetin e CH në qoftë se ka ID më të ulët.

2.3.5.5 Algoritmi i ruajtjes së energjisë i bazuar në rritjen e cluster-it (ECEC)

Në këtë algoritëm autorët kanë paraqitur një protokoll të ri të kontrollit të topologjisë që rrit jetëgjatësinë e rrjetave të mëdha ad hoc ndërkohë që sigurojnë lidhje minimale të nyjeve në rrjet, rrit aftësinë e nyjeve të arrijnë njëra tjetrën dhe kursen energjinë duke identifikuar nyjet e tepërta. [22], [29], Gjatë fazës së formimit të cluster-it, nyjet me vlerat më të larta të vlerësuara të energjisë në fqinjësinë e tyre zgjidhen si CH. Pas procesit të zgjedhjes së CH, ky algoritëm zgjedh pastaj nyjet gateway për t’u lidhur me cluster-at. Algoritmi ul konsumimin e fuqisë që çon në jetëgjatësi më të madhe të rrjetit.

2.3.5.6 Algoritmi Max-Heap Tree i bazuar në efiçencën e energjisë

Në këtë algoritëm cluster-at e vegjël të menaxhueshëm formohen duke përdorur teknikën max heap tree. Ky është një mekanizëm i përmirësuar për zgjedhjen e CH duke zgjedhur nyjen rrënjë të max-heap si CH.[23], [24] CH zgjidhet duke u bazuar në nivelin e energjisë së nyjeve ku nyja me nivel më të lartë të energjisë bëhet CH. Gjatë procesit të mirëmbajtjes së cluster-it kur një nyje e ndërmjetme largohet nga cluster-i ose CH largohet nga rrjeti është i nevojshëm balancimi i pemës, sepse kjo mund të kërcënojë

cilësitë e max-heap. Ky algoritëm përdoret për minimizimin e konsumimit të fuqisë dhe rritjen e jetëgjatësisë së rrjetit.

2.3.5.7 Algoritmi clustering bazuar në ngarkesë (WCA)

WCA bazohet në përdorimin e metrikës së kombinuar të ngarkesës që mer në konsideratë parametra të ndryshëm si niveli i nyjes, distancat me fqinjët e saj, shpejtësia e nyjes dhe koha e harxhuar si CH. [23] [28] Zgjedhja e CH bazohet në ngarkesën e çdo nyje. Në qoftë se një nyje lëviz brenda një zone që nuk mbulohet nga ndonjë CH, atëhere procedura e vendosjes së cluster-it thirret në gjithë sistemin. Për të siguruar që CH-të nuk mbivendosen përdoret një vlerë pragu e paracaktuar që tregon numrin e nyjeve që suporton çdo CH. Të gjitha nyjet në rrjet duhet të njohin ngarkesën e gjithë nyjeve të tjera para se të fillojë procesi i clustering. Si rezultat, mbingarkesa e futur nga ky algoritëm është shumë e lartë.

2.3.5.8 Algoritmti clustering i bazuar në ngarkesën fleksibël (FWCA)

Ky algoritëm përdor kombinimin e metrikave (me ngarkesa të ndryshme) për të ndërtuar cluster-at. Në procesin e zgjedhjes së CH perdoren niveli i nyjes, fuqia e mbetur e baterisë, fuqia e transmetimit dhe lëvizshmëria e nyjes. Madhësia e cluster-it nuk kalon një vlerë të paracaktuar pragu. [25], [28] Gjatë fazës së mirëmbajtjes së clusterit, ky algoritëm përdor kapacitetin e cluster-ve dhe kohë zgjatjen e lidhjes në vend të lëvizshmërisë së nyjes, pasi metrika e stabilitetit të lidhjes ndikon në zgjedhjen e CH me të njëjtën ngarkesë njëlloj si metrika e lëvizshmërisë së nyjes. Qëllimet e algoritmit janë numri i ulët i cluster-ave, mbajtja e cluster-ve të qëndrueshëm, minimizimi i numrit të thirrjeve për algoritmin dhe rritja e jetëgjatësisë së nyjeve të lëvizshme në sistem.

2.4 Aplikimet e MANET

Rrjetat mobile Ad hoc (MANET) kanë fituar popullaritet në vitet e fundit për shkak të fleksibilitetit të tyre dhe mund të vendosen në vende pa ndonjë infrastrukturë egzistuese. ose kur infrastruktura egzistuese është e shtrenjtë apo e papërshtatshme për t’u përdorur.

[4],[5] MANET lejojnë përdoruesit të aksesojnë dhe shkëmbejnë informacion pavarësisht nga pozicioni i tyre gjeografik apo afërsia me infrastrukturën. Ndryshe nga rrjetat me infrastrukturë, në MANET të gjithë nyjet janë të lëvizshme dhe lidhjet e tyre janë dinamike. Kjo ofron karakterin e decentralizuar të rrjetit si avantazh. Decentralizimi i bën rrjetet shumë fleksibël dhe të fortë. Aplikimet tipike përfshijnë:

-*Zonat ushtarake.* Pajisjet ushtarake zakonisht mbajnë disa lloje pajisjesh kompjuterike. Rrjeti ad hoc lejon ushtrinë të ketë avantazhin e teknologjisë së rrjetit të zakonshëm për të mbajtur rrjetin e informacionit ndërmjet ushtarëve, pajisjeve dhe zyrat qendrore të informacionit ushtarak. Teknikat bazë të rrjetit ad hoc vijnë nga kjo fushë.

-*Sektori komercial.* Rrjetet ad hoc mund të përdoren në raste emergjence/rreziku për ndihma në raste fatkeqësish si zjarr, përmbytje apo tërmet. Operacionet e emergjencës ndodhin kur nuk egziston infrastrukturë ose kur infrastruktura e komunikimit dëmtohet dhe është e nevojshme vendosja e shpejtë e rrjetit të komunikimit. Informacioni kalon nga një grup shpëtimi në tjetrin me një pajisje dore të vogël. Raste të tjera komerciale mund të përmendim komunikimin ad hoc ndërmjet dy anijeve etj.

-*Niveli lokal.* Rrjetat ad hoc mund të lidhin një rrjet të menjëhershëm dhe multimedia të përkohshëm duke përdorur lap top ose kompjuter personal për të përhapur dhe shpërndarë informacion ndërmjet pjesmarrësve psh. në një konferencë apo klasë. Një aplikim tjetër mund të jetë në rrjetat në shtëpi ku pajisjet mund të komunikojnë direkt për të shkëmbyer informacion. Gjithashtu këto rrjeta mund të gjejnë aplikim në mjedise të tjera civile si stadiume sportive, taxi, anije dhe aeroplanë të vegjël.

-*Rrjeti personal (PAN).* MANET mund të lehtësojnë ndërkomunikimin ndërmjet pajisjeve të ndryshme të lëvizshme si PDA, laptop dhe celular. Kabllot janë zëvendësuar me lidhjet pa tel, kështu një MANET mund të zgjerojë aksesin në internet ose rrjete të tjerë me mekanizma të tillë si: LAN pa tel (WLAN), GPRS dhe UMTS. PAN është një fushë aplikimi premtuese e MANET në kontekstin e informatikës së përhapur në të ardhmen.

- *Rrjetat me sensorë.* [6] Kjo teknologji është një rrjet i përbërë nga një numër i madh sensorësh të vegjël. Mund të përdoret për dedektimin e disa cilësive të një zone. Mund të

përmendim temperaturën, presionin, ndotjen, mbetjet toksike. Aftësitë e çdo sensori janë të limituara dhe secili duhet të mbështetet në të tjerët, në mënyrë që të përcjellë të dhënat në një kompjuter qendror. Sensorët individual janë të limituar në aftësitë e tyre llogaritëse dhe janë të prirur për dështim dhe humbje.

KAPITULLI 3

SIGURIA NË MANET

3.1 Hyrje

Rrjetat MANET kanë karakteristika të përcaktuara unike që i bëjnë ato të cënueshëm nga sulme të ndryshme. [7], [11] Meqenëse këto rrjeta vendosen në mjedis të hapur ku të gjitha nyjet bashkë veprojnë në dërgimin e paketave në rrjet, nyjet me qëllim të keq është e vështirë të dedektohen. Ndaj është e vështirë të ndërtohet një protokoll i sigurtë krahasuar me rrjetat me tel ose ato të bazuar në infrastrukturë. Për të siguruar komunikim të besueshëm në mjedise të ndryshëm, shqetësimi kryesor i rrjetave MANET është siguria e veprimeve bazë të rrjetit.

Komunikimi në rrjetat ad hoc konsiston në dy faza, zbulimi i rrugës dhe transmetimi i të dhënave. Në mjedise të kundërta, nyjet me qëllim të keq mund të ndërpresin zbulimin e rrugës duke penguar përhapjen e trafikut të kontrollit të rrugës së ligjshme dhe duke ndikuar në njohuritë topologjike të nyjeve të infektuara nga sulmi. Nyjet me qëllim të keq mund të ndërpresin dhe transmetimin e të dhënave. Së pari, ata mund të bindin zbulimin e rrugës për të vendosur veten në shtigjet e përdorur. Pastaj ata mund të ngacmojnë me të dhënat në transmetim në mënyrë arbitrare dhe të degradojnë funksionimin e rrjetit. Protokollet aktualë të rrugëzimit në MANET nuk mund të merren me ndërprerjet me qëllim të keq të transmetimit të të dhënave. Më poshtë përshkruhen tipet kryesore të sjelljes së keqe që mund të hasen në rrjet.

Nyja me sjellje të keqe

Në MANET nyje të ndryshme me sjellje të keqe formojnë sjelljen e keqe me qëllime të ndryshme. Janë dy tipe kryesorë të nyjeve me sjellje të keqe në një rrjetat ad hoc.

Nyjet me qëllim të keq, quhen ndryshe sulme, janë të aftë për rrëzim apo ndryshimin e kontrollit të paketave të të dhënave, duke parandaluar zbulimin e rrugës ndërmjet dy nyjeve, dhe bëjnë të pamundur arritjen e paketave të të dhënave në destinacionin e tyre ndërkohë që konsumojnë energji dhe gjerësi brezi të disponueshme në rrjet. Ato kanë aftësi të shkaktojnë dëme në gjithë rrjetin dhe gjithë tipet e veprimeve.

Nyjet egoiste, janë pjesë e një rrjeti ad hoc, përdorin këtë rrjet për të krijuar komunikimin e tyre. Por ato refuzojnë të harxhojnë fuqinë e tyre për veprime që nuk përfitojnë direkt prej tyre. Nyjet egoiste mund të rrëzojnë paketat e të dhënave ose të refuzojnë dërgimin e paketave të kontrollit të rrugëzimit për nyjet e tjera. Edhe pse ata nuk kanë për qëllim të dëmtojnë rrjetin, sjellja e tyre shqetëson performancën dhe ndikon në funksionimin e të gjithë rrjetit.

3.2 Aspekte të sigurisë

Për shkak të mungesës së infrastrukturës, mungesës së pajisjeve të autorizimit dhe mjedisit të shpërndarë, mekanizmat tradicional të sigurisë nuk mund të aplikohen plotësisht në një rrjet MANET. Është e vështirë të bësh nyjet e lëvizshme të vendosin një lidhje të besuar afatgjatë me çdo nyje me të cilët ato janë lidhur përkohësisht. [2]
Kjo pengon sigurimin e mbrojtjes kriptografike dhe autentikimin për të gjithë trafikun e kontrollit dhe të dhënave në rrjet. Për më tepër, edhe nëse ky lloj i shërbimeve të ishte e mundur, mbingarkesa dhe vonesa do të paraqesin një sfidë në një mjedis të tillë dinamik. Këto shërbime nuk mund të jenë efektivë kundrejt sulmit mohimi i shërbimit DoS (denial of service), në të cilin nyjet me sjellje të keqe vetëm rrëzojnë paketat e të dhënave të marra. Kështu specifikat e skemave të sigurisë në mjedisin ad hoc duhet të hetohen. Eshtë një sfidë e madhe të sigurohet komunikimi dhe mbajtja e lidhjes në prani të nyjeve me sjellje të keqe në një topologji rrjeti pa tel multihop të ndryshueshëm vazhdimisht në MANET. Në literaturë gjendet një numër i madh studimesh në lidhje me mekanizmat e sigurisë së rrugëzimit kundrejt sulmeve sipas kërkesave të ndryshme të sistemit në rrjetin ad hoc. Vetëm procedurat e rrugëzimit nuk mund të garantojnë dërgimin e sigurtë dhe të pashqetësuar të të dhënave përmes rrjetit. [11]

Kur flasim për sigurinë në përgjithësi duhen marë në konsideratë tre aspekte të rëndësishëm: kërkesat e sigurisë, sulmet e sigurisë dhe mekanizmat e sigurisë. Kërkesat e sigurisë përfshijnë funskionet e nevojshme për të siguruar një mjedis rrjeti të sigurtë, ndërsa sulmet mbulojnë metodat që mund të jenë të punësuar për të thyer këto kërkesa.

Mekanizmat e sigurië janë blloqet strukturore thelbësore të përdorur për të siguruar dhe përforcuar kërkesat e sigurisë.

Kërkesat e sigurisë: Mund të jenë një zgjidhje jetike për sulme dhe kërcënime të ndryshëm. Nqs sigurohet çelësi i sigurisë atëhere është më e lehtë të arrihet siguria. Këto kërkesa sigurie mund të implementohen në një sistem për të siguruar një nivel të lartë sigurie, por është e pamundur të implementohen të gjitha kërkesat në një sistem. Kërkuesit kanë provuar zbatimin e një sërë kërkesash të rëndësishme për të siguruar sigurinë e nevojshme për çdo sistem. Këto kërkesa përcaktohen nga unione të ndryshme të tillë si International Telecommunications Union prezantojnë rekomandimet e tyre ITU-TX.805 dhe X.800 që janë: Kontrolli i aksesit, Autentikimi, konfidencialitei i të dhënave, integriteti i të dhënave, disponueshmëria dhe privatësia.

Kontrolli i aksesit: Siguron që vetëm nyjet e autorizuar kanë leje dhe privilegjin të veprojnë në rrjet. Nyjet që marrin pjesë në rrjet duhet të kenë autorizim e duhur për të aksesuar dhe ndarë burimet, shërbimet, aplikacionet dhe të dhënat personale në këtë rrjet. Ka mënyra të ndryshme të kontrollit të aksesit: Kontrolli i aksesit diskrecional (DAC) ofron një mjet për përcaktimin e kontrollit të aksesit ndaj vetë përdoruesit. Kontrolli i aksesit i detyrueshëm (MAC) përfshin mekanizma të centralizuar për të kontrolluar aksesin e objekteve me një politikë formale të autorizimit. Kontrolli i aksesit i bazuar në funksion (RBAC) zbaton nocionin e funksioneve brenda subjekteve dhe objekteve. [12]

Autentikimi: Eshtë thelbësor për të siguruar se të dynyjet fundore janë ata që pretendojnë të jenë (të vërteta) dhe jo imitues. Pa autentikimin e duhur, asnjë kërkesë tjetër nuk mund të zbatohet në mënyrë korrekte. Psh, nqs dy nyje janë duke përdorur çelësa simetrikë enkriptimi për të shkëmbyer mesazhe të sigurtë, dhe një prej tyre kompromentohet, si rezultat i mungesës së autentifikimit të duhur, atëherë të gjitha materialet e enkriptuara si çelësat e përbashkët dhe algoritmi i enkriptimit do të jetë në dispozicion të nyjeve me sjellje të keqe. Prandaj janë të rëndësishme teknikat e autentikimit të përdoruesve në rrjetat MANET.

Disponueshmëria: Shërbimet thelbësore duhet të sigurohen nga një nyje në çdo kohë kur është e nevojshme, pavarësisht nga sulmet. Përveç kësaj, disponueshmëria e një rrjeti do

të thotë se shërbimet e tij duhet të jenë të aksesueshme, kur është e nevojshme, edhe në rast thyerje.

Konfidencialitei i të dhënave: Kjo parandalon pjesët e paautorizuara të kuptojnë përmbajtjen e mesazhit. Konfidencialiteti nuk është i kufizuar në mbijetesën e informacionit të përdoruesve, si informacione ushtarake strategjike ose taktike por gjithashtu dhe mbijetesën e informacionit të rrugëzimit. Konfidencialiteti mund të arrihet duke përdorur metodat e njohura të enkriptimit me sistemet e duhura të menaxhimit të çelësave.

Integriteti i të dhënave: Garanton që të dhënat nuk janë modifikuar, fshirë, zhvendosur gjatë transmetimit nga pjesë të paautorizuara apo sulme me qëllim të keq. Kjo është e rëndësishme në aplikime si banka, operacionet ushtarake dhe kontrollet e pajisjeve (p.sh. trena apo avionë), ku ndryshime të tilla do të mund të shkaktojnë dëme serioze.

Privatësia: Siguron që vendndodhja dhe identiteti i nyjeve mbrohen nga kundërshtari. Siguron mbrojtjen e rrjedhjes së informacionit kështu një kundërshtar nuk mund të fitojë informacionin duke e vëzhguar atë.

Janë dhe disa kërkesa të tjera që i duhen sistemit si:

Afatet kohore: Përditësimet e rrugëzimit duhet të dërgohen në kohën e duhur. Mesazhet e përditësimit që mbërrijnë me vonesë mund të reflektojnë gjendjen e gabuar të rrjetit dhe mund të çojnë në humbje të mëdha informacioni.

Izolimi: Kjo kërkon që nyjet të mund të identifikojnë nyjet me sjellje të keqe dhe të izolojnë ato. Nga ana tjetër, protokollet e rrugëzimit duhet të jetë imun ndaj nyjeve me qëllim të keq.

Llogaritje e Lehtë (lightweight): Shumë pajisje të lidhura me një ad hoc supozohet të jenë me bateri me aftësi të kufizuar kompjuterike. Ata nuk mund të jenë në gjendje të kryejnë algoritme të mëdha kriptografike.

Vetë-stabilizimi: Nyjet duhet të jenë në gjendje të marrin veten nga sulmet në mënyrë të pavarur në kohë reale pa ndërhyrjen e njeriut. Nëse nyjet janë të vetë-stabilizuara në sulmet me qëllim të keq, atëherë sulmuesi do të mbetet në rrjet, dhe do të vazhdojë

dërgimin e mesazheve të gabuara në mënyrë që të rrëzojë sistemin, por do të jetë më e lehtë për nyjet të gjejnë sulmuesin.

Mbijetesa: Kjo është aftësia e sistemit për të përmbushur misionin e saj në kohën e duhur, në prani të aksidenteve, dështimeve, ndërhyrjeve apo sulmet me qëllim të keq. Misioni do të thotë restaurimi dhe mirëmbajtja e shërbimeve thelbësore, gjatë dhe pas sulmit, edhe në qoftë se një pjesë e madhe e sistemit është dëmtuar ose shkatërruar.

Anonimati: As nyja dhe as sistemi nuk duhet të ekspozojë informacion si adresën MAC dhe adresat IP, të cilat mund të vënë sistemin në rrezik.

3.4 Kërcënimet ndaj rrjetave MANET

Rrjetat MANET duhet të sigurojnë nivele të ndryshme të sigurisë për aplikime të ndryshme për vendosjen dhe përdorimin e sukseshëm të tyre. [12] Megjithatë, për shkak të lidhjeve të tyre pa tel dhe mungesës së administratës qendrore, rrjetat MANET kanë shqetësime më të mëdha të sigurisë se rrjetat konvencionale. Për shembull, është e lehtë për sulmuesit të futen ose të lënë një rrjet pa tel dhe të përgjojnë atë, duke qenë se nuk ka lidhje fizike. [10]

Pa vendosjen e një skeme sigurie, një nyje e jashtme mund të pretendojë të bëhet një nyje e brendshme dhe të marrë pjesë në rrugëzimin e paketave, ngatërrimin e tyre, injektimin e paketave false ose të shkaktojë mbingarkesë në rrjet.

Ka lloje të shumta të sulmeve në rrjetat mobile ad hoc të cilët klasifikohen:

Duke u nisur nga burimi i sulmeve ndahen në:

Sulme të jashtëm: Sulmuesi ka si qëllim të krijojë mbipopullim, të përhapë informacione rrugëzimi të falsifikuara ose të shqetësojë nyjet gjatë kryerjes së shërbimeve.

Sulme të brendshëm: Ky është një sulm në të cilin sulmuesi dëshiron të fitojë akses normal në rrjet dhe të marrë pjesë në aktivitetet e rrjetit me disa imitime me qëllim të keq që të ketë akses në rrjet si një nyje e re, ose duke kompromentuar direkt një nyje të rrjetit dhe duke e përdorur atë si bazë për të kryer sjelljen e tij me qëllim të keq. Këto sulme janë paraqitur skematikisht në figurën 3.1

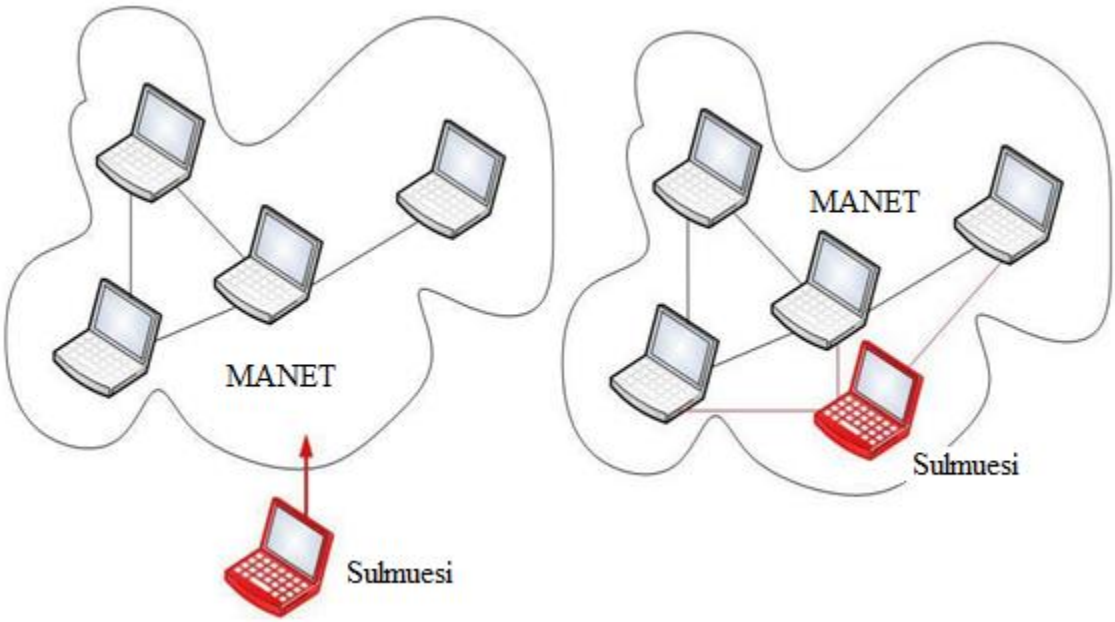


Figura 3.1. Sulmet e jashtëm dhe të brendshëm

Duke u bazuar në sjelljen e tyre kemi: Sulme pasivë dhe aktivë.[13]

Sulmet pasivë nuk ndryshojnë paketat e të dhënave ose modifikojnë ndonjë veprim për kontrollin e paketave. Ato vetëm dëgjojnë gjatë transmetimit pa i modifikuar paketat. Sulmuesi kërkon të jetë në zonën radio të nyjes për të dëgjuar. Ky lloj sulmuesi ka si qëllim konfidencialitetin e të dhënave. Zbulimi i këtij tipi sulmi është i vështirë duke qenë se ai nuk ndryshon ndonjë gjë. Një zgjidhje është përdorimi i metodave të fuqishme të enkriptimit për të enkriptuar të dhënat që do të trasnmetohen.

Në sulmet aktivë nyja sulmuese ndërhyn kundër veprimeve të rrjetit. Ky sulm mund të ndikojë në rrugëzimin e rrjetit, numërimin e hop-ve, leximin e të dhënave duke i alternuar ato apo duke falsifikuar IP e nyjes. Ndërsa gjatë transmetimit ky sulm vepron duke rrëzuar paketën, lexuar dhe modifikuar paketat. Dedektimi i këtij sulmi është më i lehtë duke qenë se mund të bëhen disa alternime të funksioneve të rrjetit. Shembull i këtyre sulmeve jepet në figurën 3.2.

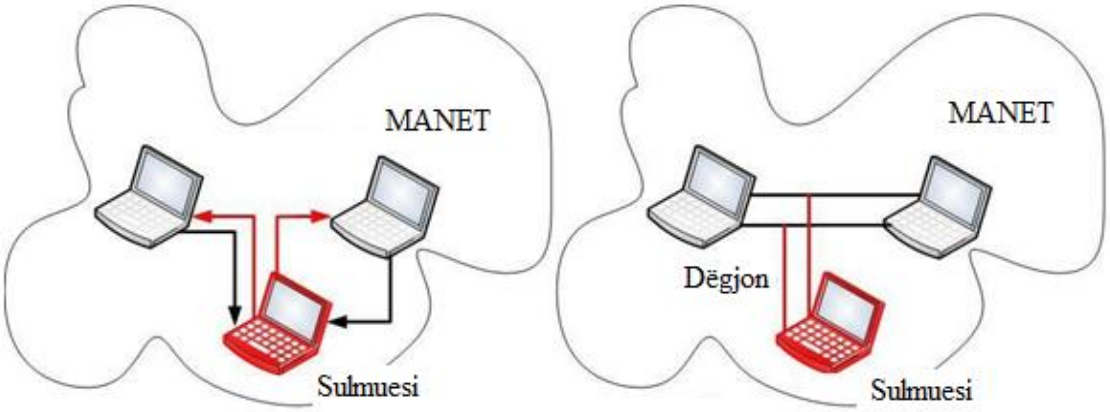


Figura 3.2. Sulmi aktiv dhe pasiv në MANET

Sulmet aktive mund të ndahen në katër kategori:

Sulmet e Dropping, Këtu paketat e të dhënave që janë transmetuar bien në nyjen e kompromentuar ose egoiste.

Sulmet e modifikimit, këtu sulmet alternojnë paketat dhe ndërpresin komunikimin ndërmjet nyjeve në rrjet.

Sulmet e fabrikimit, nyja sulmuese dërgon mesazhe false pa marrë mesazhe dhe mund të quhet si përgjigje e falsifikuar.

Sulmet timing, këtu sulmuesi sulmon nyjet e tjera për të shfaqur veten si nyje e afërt me nyjen aktuale, për të treguar që ka një rrugë mjaftueshëm të freskët për destinacion.

Sulmet gjithashtu mund të klasifikohen sipas stack-ut të protokollit të rrjetit, disa sulme mund të hasen në shumë shtresa.

Rrjetat MANET kanë pesë shtresa:

Shtresa e aplikimit: Përcakton protokollet e aplikimit dhe se si hostet programojnë ndërfaqen me shtresën e transportit për të përdorur rrjetin.

Shtresa e transportit: Përcakton nivelin e shërbimit dhe statusin e lidhjes së përdorur kur transmetohen të dhëna.

Shtresa e rrjetit: Paketon të dhënat në datagrame IP dhe kryen rrugëzimin e datagrameve IP.

Shtresa e linkut të të dhënave: Siguron transferimin e frameve të të dhënave pa gabime nga njëra nyje te tjetra.

Shtresa fizike: Ka të bëjë me transmetimin dhe pranimin e rrjedhjes së pastrukturuar të biteve në një mjedis fizik.

Sulmet e shtresës fizike

Përgjimi është kapja dhe leximi i mesazheve dhe bisedave nga marrës të paparamenduar.

Mesazhet e transmetuara mund të përgjohen dhe mund të injektohen mesazhe false në rrjet. Për më tepër, një sinjal radio mund të bllokohet ose interferohet duke shkaktuar korruptimin ose humbjen e mesazhit.[14]

Sulmet e bllokimit mund të kalojnë nga një vendndodhje e largët në rrjetin e shënjestruar. Këtu përfshihet dhe interfernca aktive që është gjithashtu një sulm i mohimit të shërbimit i cili shtrembëron komunikimin.

Sulmet e shtresës së linkut

Sulmet mund të synojnë shtresën e linkut duke ndërprerë bashkëpunimin e protokolleve të shtresës. Përfshihen tre tipe sulmesh.

Sjellja egoiste e nyjeve: Këto janë nyje egoiste që rrëzojnë qëllimisht paketat për të kursyer fuqinë e baterisë ose për të parandaluar pjesë të padëshiruara të gjerësisë së brezit.

Sjellja me qëllim të keq e nyjeve: Ato ndërpresin veprimin e protokollit të rrugëzimit dhe efekti i tyre është i konsiderueshëm kur vendosen disa komunikime ndërmjet nyjeve fqinje.

Analiza e trafikut: Këtu sulmet analizojnë rrjedhjen e trafikut për të marrë informacion të rëndësishëm mbi topologjinë e rrjetit që në kthim të zbulojë informacionin rreth nyjeve.

Sulmet e shtresës së rrjetit

Duke sulmuar protokollet e rrugëzimit, sulmet mund të përthithin trafikun e rrjetit, injektojnë veten në rrugën ndërmjet burimit dhe destinacionit dhe kështu kontrollojnë rrjedhjen e trafikut. [14] Paketat e trafikut mund të dërgohen në një rrugë jo optimale, që mund të fusë vonesa të dukshme. Përveç kësaj paketat mund të dërgohen në një rrugë jo egzistuese dhe humbet. Sulmuesit e shumëfishtë mund të pengojnë një nyje burim të gjejë

një rrugë për në destinacion duke shkaktuar ndarjen e rrjetit në pjesë, që shkakton trafik kontrolli të tepërt të rrjetit dhe shpejton degradimin e performancës.

Ka disa sulme rrugëzimi me qëllim të keq që synojnë zbulimin e rrugëzimit ose fazën e mirëmbajtjes duke mos ndjekur specifikimet e protokolleve të rrugëzimit, si sulmet e rrjedhjes së mesazhit të rrugëzimit, rrjedhja e mesazhit Hello, RREQ, ACK, dyndje e tabelës së rrugëzimit, loop i rrugëzimit etj.

Sulmet e shtresës së transportit

Rrjetat MANET janë të kërcënuar nga sulmi klasik rrjedhja SYN (flooding) dhe sulmet e rrëmbimit të sesionit. Kështu një MANET ka një normë më të lartë gabimi të kanalit krahasuar me rrjetat me tel. [11] Ky sulm është një sulm i mohimit të shërbimit. Sulmuesi krijon një numër të madh lidhjesh gjysmë të hapura TCP me një nyje viktimë, por nuk e plotëson asnjëherë "handshake" për hapjen e plotë të lidhjes. Gjatë sulmit, një nyje me qëllim të keq dërgon një sasi të madhe paketash SYN drejt nyjes viktimë, duke falsifikuar adresat e kthimit të paketave SYN. Në tip tjetër sulmi është rrëmbimi i Sesionit. Ky sulm merr përparësi nga fakti që shumica e komunikimeve janë të mbrojtura në ndërtimin e sesionit, por jo pas kësaj. Në sulmin e rrëmbimit të sesionit TCP, sulmuesi falsifikon adresën IP të viktimës, përcakton numrin e saktë të sekuencës që pritet nga objektivi dhe pastaj kryen një sulm DoS mbi viktimën. Kështu sulmuesi luan rolin e nyjes viktimë dhe vazhdon sesionin me objektivin e tij.

Sulmet e shtresës së aplikimit

Mund të jenë viruse të lëvizshëm, sulmet worm dhe sulmet e mospranimit.

Sulmet e virusit të lëvizshëm dhe sulmet worm: Në rrjeta ka disa teknika me anë të të cilave një worm zbulon makina të reja për të shfrytëzuar. Një shembull është skanimi i adresës IP i përdorur nga worm e internetit. Kjo teknikë konsiston në gjenerimin e paketave të kontrollit në portën e kërcënuar UDP/TCP në disa adresa IP të ndryshme. Hostet e prekur nga përgjigja e skanimit marrrin një kopje të worm, dhe kështu infektohen.

Sulmi i mospranimit: Mospranimi i referohet mohimit të pjesmarrjes në gjithë komunikimet ose në një pjesë të tyre.

Sulme të tjerë të avancuar

Sulmi Wormhole: Sulmuesi njeh paketat në një vendndodhje të rrjetit dhe i kanalizon ato në një vendndodhje tjetër. Rrugëzimi mund të ndërpritet kur kanalizohen mesazhet e kontrollit të rrugëzimit. Ky kanal ndërmjet dy sulmuesve të lidhur quhet wormhole. [16] Sulmet wormhole janë kërcëcine të ndryshme në protokollet e rrugëzimit në MANET. Psh, kur sulmi përdoret kundër protokolleve sipas kërkesës si DSR apo AODV, sulmi mund të pengojë zbulimin e ndonjë rruge tjetër.

Sulmi Blackhole: Sulmi blackhole ka dy karakteristika: Së pari, nyja shfrytëzon protokollin e rrugëzimit, të tillë si AODV, për të shfaqur veten sikur ka një rrugë të vlefshme për në nyjen destinacion, edhe pse rruga është false, me qëllim të ndërprerjes së paketave. Së dyti, sulmuesi konsumon paketat e ndërprera pa i dërguar ato. Megjithatë sulmi shton rrezikun që nyjet fqinje të monitorojnë dhe të vënë në dukje sulmet në vazhdim. Kjo është një formë e lehtë e këtyre sulmeve kur një sulmues dërgon paketat në mënyrë selektive.

Sulmi Byzantine: Një nyje e kompromentuar e ndërmjetme punon e vetme, ose disa nyje të ndërmjetme të kompromentuara punojnë së bashku dhe mbartin sulme të tillë si krijimi i loop-ve të rrugëzimit, dërgimi i paketave nëpërmjet rrugëve jo optimale, ose rrëzojnë paketa në mënyrë selektive, që rezulton në ndërprerjen ose degradimin e shërbimeve të rrugëzimit.

Sulmi i nxitimit: Dy sulmues të lidhur përdorin procedurën e kanalizimit për të formuar një wormhole. Nqs një rrugë e shpejtë transmetimi (psh. një kanal i përbashkët i dedikuar nga sulmuesit) egziston ndërmjet dy wormhole fundorë, paketat e kanalizuara mund të përhapen më shpejt sesa nëpërmjet një rruge normale multi-hop. Kjo formon sulmin e nxitimit (rushing). Ky sulm mund të veprojë si një sulm efektiv mohimi i shërbimit kundër gjithë protokolleve të rrugëzimit sipas kërkesës në MANET, përfshirë dhe protokollet që janë ndërtuar të jenë të sigurtë të tillë si ARAN, ARIADNE etj.

Sulmi i konsumimit të burimeve: Njihet dhe si sulmi sleep deprivation. Sulmuesi ose nyja e kompromentuar përpiqet të konsumojë baterinë duke kërkuar zbulimin e rrugëve shtesë, ose duke dërguar paketa të panevojshme në nyjen viktimë.

Sulmi i zbulimit të vendndodhjes: Një sulmues zbulon informacion në lidhje me vendndodhjen e nyjeve ose strukturën e rrjetit. Ajo mbledh informacion për vendndodhjen e nyjes, të tilla si një hartë rruge, dhe pastaj planifikon skenarë të mëtejshëm sulmi. Analiza e trafikut, një nga sulmet më delikat kundër MANET nuk është zgjidhur. Kundërshtarët përpiqen të kuptojnë identitetin e palëve të komunikimit dhe të analizojnë trafikun për të mësuar modelin e trafikut të rrjetit dhe ndryshimet e rrugës në modelin e trafikut. Rrjedhja e një informacioni të tillë është shkatërruese në skenarët e ndjeshëm të sigurisë.

Sulmet në disa shtresa

Këtu përfshihen sulme të tillë si: Mohimi i shërbimit DoS, man in the middle dhe sulmet e imitimit.

Mohimi i shërbimit: Mund të nisen nga shtresa të ndryshme. Një sulmues mund të fuse një bllokim sinjali në shtresën fizike që shtesëson komunikimet normale. Në shtresën e linkut, nyjet me qëllim të keq mund të okupojnë kanalet nëpërmjet efektit të kapjes, dhe pengon nyjet e tjera nga aksesi i kanalit. Në shtresën e rrjetit, procesi i rrugëzimit mund të ndërpritet nëpërmjet modifikimit të paketës së kontrollit, rënies selektive, mbingarkesës së tabelës apo helmimit. Në shtresën e transportit dhe të aplikimit, rrjedhja SYN, rrëmbimi i sesionit dhe programet me qëllim të keq mund të shkaktojnë sulmet DoS.

Sulmet e imitimit: Këto sulme janë vetëm hapi i parë i disa sulmeve, dhe përdoren për të filluar sulme të mëtejshme të sofistikuara. Për shembull, një nyje me qëllim të keq mund t'i paraprijë një sulmi duke alternuar adresën e saj MAC ose IP.

Sulmet Man-in-the-middle: Sulmuesi vendoset ndërmjet dërguesit dhe marrësit dhe dëgjon informacionin ndërmjet dy fundorëve. Në disa raste sulmuesi mund të luajë rolin e dërguesit për të komunikuar me marrësin ose luan rolin e marrësit për t’ju përgjigjur dërguesit.

3.4.1 Kufizimet dhe kërcënimet në rrugëzimin bazuar në clustering

Egzistojnë disa algoritme dhe përmirësime për protokollet e bazuar në cluster, por shumë pak trajtojnë çështjen e sigurisë. Këto algoritme arrijnë bashkëpunimin ndërmjet

nyjeve. Por në qoftë se nuk marim parasysh supozimin se të gjitha nyjet janë jo me qëllim të keq, bashkëpunuese dhe të e besueshme dhe të vlerësohet situata, vihet re që ka një parregullsi në rrjet. Ana negative e skemës së përmendur është se nuk mer në konsideratë çështjen e egoizmit, ligësisë dhe të sigurisë, të cilat ndikojnë ndjeshëm në performancën e rrjetit Ad hoc [21].

Struktura e rrjetit ad hoc është e tillë që aktualisht nuk mund t'u besohet të gjithë pjesëmarrësve. Si pasojë, në një mjedis si rrjeti ad hoc nuk mund të lihen mënjanë këto çështje.

Të gjitha nyjet e cluster-it në rrugëzimin e bazuar në cluster mbështeten në nyjen CH (cluster head) për zbulimin dhe menaxhimin e rrugës. Në qoftë se nyja CH sillet me keqdashje, atëhere do të dëmtohet i gjithë mekanizmi i zbulimit të rrugës dhe mirëmbajtjes. Kur një nyje CH bëhet me qëllim të keq:

• Ajo mund të pranojë kërkesat për rrugë, por nuk mund të përgjigjet

• Ajo pranon informacionin e rrugës nga CH-t dhe nyjet e tjera por nuk përgjigjet.

• Ajo i përgjigjet në mënyrë selektive kërkesave të ndryshme, dhe jo të gjithave.

• Nuk e përditëson listën e rrugëzimit dhe fsheh rilidhjet.

• Ajo mund të çkyçet sa herë që dëshiron pa marrë në konsideratë lidhjet dalëse.

• Ajo mund të luajë me mesazhet duke fshirjë shërbimet legjitime, duke futur mesazhe false ose duke bërë ndryshime në mesazhet egzistuese.

• Kjo mund të çojë në mosnjohje, dmth mohon kryerjen e disa detyrave të veçanta në fjalë

• Nyja CH mund të çojë në sulmin e mohimit të shërbimit pasi ajo ka autoritetin për të lejuar (ose jo) shërbimet.

Sulmet në rrugëzimin bazuar në clustering

Siguria e komunikimit në MANET është shumë e rëndësishme për transmetimin e sigurtë të të dhënave. Mungesa e mekanizmit qendror koordinues i bën MANET të prirur ndaj sulmeve dixhital / kibernetike. Këto sulme mund të jenë një CH, mund të veprojë në rrugëzimin inter-cluster, në transmetimin e informacionit etj. Në varësi të ndikimit që kanë nyjet me qëllim të keq në cluster, sulmet ndahen në sulme direkt në cluster ose

indirekt. Në sulmin direkt, nyjet me qëllim të keq pengojnë procedurën e përzgjedhjes së CH, që e bën të vështirë krijimin e cluster-ve. Prandaj, është i pamundur krijimi i rrugëzimit në clustera. Ky lloj sulmi shkatërron komunikimin brenda rrjetit. Sulmet flooding dhe rushing janë sulme tipike direkte në clustering. Për të plotësuar sulmin indirekt në cluster, fillimisht të gjitha nyjet me qëllim të keq duhet të zgjidhen si CH me avantazhin e metrikave false gjatë procedurës së zgjedhjes së cluster head-it. Pas kësaj, këto CH me qëllim të keq do të kryejnë sulme të ndryshëm në rrugëzim. Krahasuar me sulmin direkt, sulmi indirekt është më i vështirë për t'u dedektuar. Sulmi wormhole është një shembull i këtij sulmi. Në cluster, sulmuesit janë të suksesshëm të bëhen nyje gateway, dhe kështu ato sulmojnë rrjetin duke qenë se janë nyje kyçe. [22]

Protokollet e formimit të cluster-it verifikojnë një mënyrë për t'i bërë nyjet grup dhe disa prej tyre më efektive të bëhen si cluster head. Çdo protokoll përdor një funksion të veçantë të shërbimeve të mbështetur në disa metrika (niveli i nyjes, kohëzgjatja e baterisë, lëvizshmëria e nyjes). Zgjedhja e nyjeve të përshtatshme për CH kërcënohet kryesisht nga: (1) sulmet egoiste në të cilët nyjet mashtrojnë në mënyrë që të mos zgjidhen CH dhe për të mbajtur energjinë dhe gjerësinë e brezit për veten e tyre, dhe (2) sulmet greedy në të cilët nyjet mashtrojnë për t'u zgjedhur CH dhe të kenë akses në të dhënat e vlefshme të rrjetit dhe të menaxhojnë trafikun e anëtarëve të cluster-it të tyre.

Për të shmangur këto, zgjedhja e CH duhet të jetë e drejtë (dmth nyja e zgjedhur duhet të jetë ajo që maksimizon dobishmërinë) dhe gjithashtu rolet duhet të ndërrohen.

3.5 Mekanizmat e sigurisë

Siguria është shërbimi thelbësor për komunikimet në rrjetat me tel dhe pa tel. Suksesi i MANET varet shumë nëse siguria e tij mund të arrihet. Megjithatë, karakteristikat e MANET paraqesin të dyja sfidat dhe mundësitë në arritjen e qëllimeve të sigurisë, të tilla si konfidencialiteti, vërtetimi, integriteti, disponueshmëria, kontrolli i aksesit, dhe jo-mospranimi. [11]

Hostet e lëvizshëm që formojnë një MANET janë pajisje normale të lëvizshme me burime dhe mbrojtje fizike të kufizuar. Karakteristikat dhe natyra e MANET kërkojnë

bashkëveprim strikt të hosteve pjesmarrës në rrjet. Egzistojnë në literaturë teknika të ndryshme sigurie dhe janë propozuar një sërë protokollesh sigurie për të përforcuar bashkëpunimin dhe penguar sjelljen e keqe, të tillë si 802.11 WEP, IPsec, SEAD, SAODV, SRP, ARAN, SSL, ARIADNE etj. Megjithatë asnjë nga këto metoda nuk është e përkryer ose e aftë të mbrojë kundër gjithë sulmeve. Një linjë e dytë e mbrojtjes e quajtur sistemet e dedektimit të ndërhyrjeve (IDS) është propozuar dhe aplikuar në MANET. IDS janë disa nga mjetet e fundit të sigurisë në betejën kundër sulmeve. IDS e shpërndara u prezantuan në MANET për të monitoruar sjelljen e keqe apo egoizmin e hosteve ushtarake.

Janë zbuluar një sërë mekanizmash sigurie kundër sulmeve me qëllim të keq. Teknikat konvencionale të tilla si autentikimi, kontrolli i aksesit, enkriptimi dhe nënshkrimi dixhital përbëjnë linjën e parë të mbrojtjes. Si linjë e dytë e mbrojtjes janë implementuar në MANET sistemet e dedektimit të ndërhyrjeve dhe mekanizma të përforcimit të bashkëpunimit që ndihmojnë në mbrojtjen kundër sulmeve.

- *Mekanizmi Parandalues:*

Skemat konvencionale të autentikimit dhe enkriptimit bazohen në kriptografi, që përfshin kriptografinë simetrike dhe asimetrike. [14] Shembuj të kriptografisë të tillë si funksionet hash përdoren për të rritur integritetin e të dhënave në transmetim. Kriptografia prag përdoret për të fshehur të dhënat nga ndarja në një numër me presje. Nënshkrimi dixhital përdoret për të arritur integritetin e të dhënave dhe autentikimin. Gjithashtu është e nevojshme të konsiderohet siguria fizike e pajisjeve të lëvizshme, meqenëse hostet janë pajisje të vogla inteligjente (smart), dhe të kërcënuara fizikisht. Psh, një pajisje mund të vidhet lehtësisht, të humbë apo të dëmtohet. Mbrojtja e të dhënave në një pajisje fizike mund të përforcohet nga disa module sigurie, si kartat smart apo me shenjë që aksesohen me PIN, çelës ose biometrike. Të kombinuar këto teknika mund të pengojnë shumë sulme në teori, ndërsa në praktikë ka një numër sulmesh që i anashkalojnë mekanizmat e sigurisë.

- *Mekanizmat reaktive*

Sistemet e dedektimit të ndërhyrjeve përdoren gjerësisht për dedektimin e anomalive dhe keqpërdorimit. Një sistem dedektimi i keqpërdorimit përpiqet të përcaktojë sjelljen e parregullt të bazuar në modelet e sulmeve të njohur, por i mungon aftësia e dedektimit të sulmeve që nuk konsiderohen gjatë krijimit të modelit. Dedektimi i anomalive përpiqet të përcaktojë sjelljen e parashikuar ose normale në mënyrë statistikore. Ai lidh të dhënat nga sjellja e rregullt e përdoruesit në një periudhë kohe, dhe pastaj teston në mënyrë statistikore për përcaktimin e sjelljes anormale me një nivel të lartë konfidence. Në praktikë, të dy teknikat mund të kombinohen që të rrisin efikasitetin kundër sulmeve.

3.6 Siguria e rrugëzimit në MANET

MANET kanë karakteristika të caktuara në menaxhimin e çelësit për shkak të mungesës së infrastrukturës, mungesës së ruterave të dedikuar, nyjeve të lëvizshme, fuqisë së baterisë të kufizuar, gjerësisë së brezit dhe memories [14] [16]. Kërkesa kryesore e sigurisë në MANET është një protokoll rrugëzimi i sigurtë i cili të ketë aftësinë të dedektojë nyjet me qëllim të keq, të garantojë procesin e zbulimit të rrugës së saktë, të mbajë informacionin e topologjisë së rrjetit konfidencial dhe të jetë i qëndrueshëm ndaj sulmeve. Janë propozuar një sërë zgjidhjesh për sigurinë. Më poshtë jepen disa prej tyre.

3.6.1 Protokoll rrugëzimi ad hoc i sigurtë (SAR)

Qëllimi i SAR është mbrojtja e informacionit ose sjelljes që mund të shkaktojë një ndryshim në tabelat e rrugëzimit në nyjet bashkëpunuese të përfshira në protokollin e rrugëzimit. [13], [16]

Bazohet në protokollet e rrugëzimit sipas kërkesës si AODV ose DSR. Në protokollin origjinal nqs një nyje dëshiron të dërgojë informacion në nyjet e tjera ajo dërgon një paketë kërkesë rruge tek fqinjët e saj dhe merr një paketë përgjigje RREP në kthim që tregon rrugën më të shkurtër për në destinacion. Në shumë protokolle rrugëzimi qëllimi kryesor është zbulimi i rrugës më të shkurtër për në destinacion duke konsideruar vetëm gjatësinë e rrugës. Por SAR përfshin një metrikë sigurie në paketën RREQ, kështu që dhe ndryshimi i veprimit të dërgimit varet nga RREQ. Kurdo që merret një paketë RREQ nga

një nyje e ndërmjetme, SAR sigurohet që nyja mund ta përpunojë paketën ose ta dërgojë atë vetëm nqs nyja ka autorizimin e kërkuar. Paketa RREP bie nqs nyja nuk e ka këtë autorizim. E meta e SAR është që nuk garanton që rruga e zbuluar nga SAR ndërmjet burimit dhe destinacionit është më e shkurtra, por gjen rrugën që garanton siguri dhe kërkon çelësa të ndryshëm për nivele të ndryshme duke rritur numrin e çelësave. SAR nuk është i aftë të gjejë rrugën më të shkurtër sepse të gjithë nyjet në rrugën më të shkurtër mund të mos kënaqin kërkesat e sigurisë. Nqs të gjithë nyjet në rrugën më të shkurtër i kënaqin këto kërkesa atëhere SAR mund të gjejë rrugën më të shkurtër.

3.6.2 Protokoll rrugëzimi vektor distance efikas i sigurtë (SEAD)

Është projektuar kryesisht për DSDV (Vektor distancë me renditje destinacioni). [13] SEAD ofron një protokoll të fuqishëm kundër sulmuesve duke u përpjekur të krijojë gjendje rrugëzimi të pasaktë në nyjen tjetër. Ky protokoll mund të anashkalojë mohimin e shërbimit, gjithë llojet e sulmeve të rrugëzimit dhe të konsumimit të burimeve. Ai përdor funksionin hash me një mënyrë pa përdorur mekanizmin e kriptografisë asimetrike. Përdor zingjirin hash për autentikimin e numërimit të hopeve dhe numrave të sekuencës. Mekanizmi përdor autentikimin për të diferencuar nyjet me qëllim të keq nga ato jo me qëllim të keq, që në kthim ulin konsumimin e burimeve nga sulmet e futur nga nyjet me qëllim të keq. SEAD shmang loopet e rrugëzimit, por pengesa qëndron kur sulmuesi përdor të njëjtën metrikë dhe numër sekuence të përdorur për autentikimin. Për të zbuluar rrugën më të shkurtër ky protokoll përdor një version të algoritmit të shpërndarë Bellman Ford. Ky mekanizëm mund të përdoret dhe në protokolle të tjerë vektor distancë.

3.6.3 Protokoll i sigurtë sipas kërkesës për MANET (ARIADNE)

Është një protokoll rrugëzimi i sigurtë bazuar në kërkesë i cili propozon një mekanizëm për mbrojtjen ndaj sulmeve të rrugëzimit dhe mohimit të shërbimit. [18] Ky protokoll përdor çelësat MAC dhe të përbashkët ndërmjet nyjeve për të siguruar autentikimin ndërmjet tyre dhe përdor time stamp për jetëgjatësinë. Përbëhet nga dy faza: faza e zbulimit të rrugës dhe mirëmbajtja e rrugës. Në fazën e parë nyja burim krijon një rrugë duke dërguar paketa kërkese rruge (RREQ) të cilët përmbajnë adresën IP të burimit dhe

destinacionit. Mirëmbajtja e rrugës kryhet kur vihet re një rënie e linkut në një nyje të rrugës për në destinacion. Në këtë rast linku i rënë nuk do të pranojë paketat e trasnmetuara nga nyja fqinje, dhe nyja dërgon një mesazh gabimi (RERR) tek nyja burim. ARAN pengon sulmet e falsifikimit me time stamps. Përdorimi i rrugës së burimit pengon loop-et meqenëse paketat kalojnë vetëm nëpërmjet nyjeve të ligjshme, dhe nuk mund të krijojnë loop-e gjatë time stamp. Sulmet wormhole janë të mundshëm në këtë protokoll ndërmjet dy nyjeve të kompromentuara.

3.6.4 Rrugëzim i autentikuar për rrjetat ad hoc (ARAN)

Propozuar nga Sanzgiri, është një protokoll sigurie që bazohet në certifikatat kriptografike që kapërcen të gjitha llojet e sulmeve në shtresën e rrjetit. Tre karakteristikat kryesore të kriptografisë si autentikimi, integriteti dhe non-repudation mbështeten nga protokollet AODV dhe DSR. [10] Edhe pse ky mekanizëm është mjaft i fuqishëm kundër sulmeve, ai bazohet kryesisht në koordinimin paraprak të sigurisë përmes nyjeve që nuk mund të jenë gjithmonë të sakta. Çështja e një çertificate false në një nyje kërcënon non-repudation dhe autentikimin. ARAN përdor kriptografinë asimetrike për të siguruar rrugëzimin në rrjetat ad hoc dhe kërkon palën e tretë të sigurisë universal (T). Konsiston në tre faza operacionale të përcaktuara: faza e parë është procesi paraprak i çertifikimit që kërkon ekzistencën e një auteriteti të çertificatës të besuar (CA). Faza e dytë është procesi i zbulimit të rrugës që siguron autentikimin fund më fund. Kjo siguron që destinacioni i synuar të arrihet me të vërtetë. Faza e tretë është opsionale dhe siguron që është zbuluar rruga më e shkurtër. ARAN përdor kriptografinë e çelësave publik dhe serverin e autoritetit qendror të çertifikimit për autentikimin e nyjeve dhe nyjeve fqinjë në zbulimin e rrugës. Ai pengon sulmet e falsifikimit si dhe disa sulme të përsëritjes. Por mund të kërcënohet nga sulme si mohimi i shërbimit apo sulmi wormhole dhe blackhole.

3.6.5 Dedektimi, parandalimi dhe reagimi i AODV

Siguron një mekanizëm kundër sulmit blackhole. Zbulon nyjet me qëllim të keq dhe i izolon ato nga dërgimi i të dhënave aktive dhe nga rrugëzimi. Reagon duke dërguar

paketa Alarm te fqinjët e saj. Ky protokoll përdor një përditësim dinamik të vlerës së pragut. Në rrugëzimin normal si AODV paketa RREP pranohet vetëm nqs ajo ka numrin e sekuencës së destinacionit më të lartë se ai në tabelën e rrugëzimit.[17] DPRAODV kontrollon nëse numri i sekuencës së destinacionit është më e lartë se vlera prag apo jo. Nqs është më e lartë atëhere nyja është nyje me qëllim të keq dhe shtohet në listen e zezë. Pastaj fqinjët e kësaj nyje njoftohen duke dërguar një paketë kontrolli të quajtur ALARM. Parametrat e paketave ALARM janë nyjet e listës së zezë. Kështu nqs nyja merr paketën nga lista e zezë ajo thjesht e hedh paketën RREP. Ajo gjithashtu bllokon përgjigjet e përsëritura nga nyja me qëllim të keq duke zvogëluar trafikun e rrjetit dhe duke izoluar nyjet me qëllim të keq nga rrjeti.

3.6.6 Bashkëpunimi i nyjeve: Drejtësia në MANET Dinamik (CONFIDANT)

Është një skemë mospranimi që ka si qëllim dedektimin dhe izolimin e nyjeve me sjellje të keqe. Punon si zgjerim i protokolleve reaktive të tillë si DSR. [14] Nyjet monitorojnë sjelljen e fqinjëve një hop larg tyre. Duke mbajtur një kopje të paketës gjatë dëgjimit të ritransmetimit të nyjes tjetër, mund të dedektohen veprimet me qëllim të keq si ndryshimet në përmbajtjen e mesazhit dhe paketat e rëna. Kur një numër prag ngjarjesh të dyshimta dedektohen nga një nyje, nyja monitoruese njofton nyjet fqinje rreth sjelljes së dyshuar. Nqs është i mjaftueshëm evidentimi i nyjes si nyje me qëllim të keq, ajo lihet pas dore në zbulimin e rrugës.

3.6.7 Protokoll i sigurtë rrugëzimi me ndihmën e pozicionit (SPAAR)

Ky protokoll mbron një MANET nga sulmet e nyjeve me qëllim të keq, duke u përpjekur të minimizojë potencialin e demtimit nga sulmet e kryer nga nyjet e kompromentuara.

Një parakusht i domosdoshëm për SPAAR është që çdo pajisje është e aftë të përcaktojë vendndodhjen e saj [13], [16]. Tabelat e rrugëzimit mbajnë informacion rreth identitetit të nyjes, vendndodhjes, rendit të transmetimit dhe shpejtësisë. Informacioni i pozicionit fshihet nga nyje të paautorizuara. Për numërimin e sulmeve wormhole dhe nyjes së padukshme, mesazhet e rrugëzimit pranohen vetëm nga fqinjët 1 hop të verifikuar.

SPAAR mbështetet në kriptografinë asimetrike. Çdo nyje gjeneron një çift çelësash enkriptimi/dekriptimi të grupit private/publik për fshehjen e përmbajtjes së RREQ dhe mesazheve të tjerë të dërguar. Çelësi publik i dekriptimit i grupit shpërndahet në gjithë fqinjët e enkriptuar të verifikuar sipas çelësave publikë respektivë. RREQ enkriptohen hap pas hapi me ndihmën e çelësit publik të nyjes pasardhëse të dërgimit. Mbrojtja hap pas hapi ka ngjashmëri me ARAN. Ndërsa ARAN siguron vetëm integritetin dhe autenticitetin, SPAAR siguron konfidencialitetin hap pas hapi.

3.6.8 AODV bazuar në metodën e autentikimit kriptografik (SAODV)

Metoda e propozuar bazohet në protokollin e rrugëzimit AODV dhe përdor teknologjinë e çelësit sekret të përbashkët. [17] Në AODV mesazhet e rrugëzimit RREQ dhe RREP kanë dy tipe informacioni: të ndryshueshëm dhe jo të ndryshueshëm. Numri i hopeve është fusha e ndryshueshme duke qene se nyja e ndërmjetme e rrit atë kur transmeton RREQ. Fushat e tjera si numri i sekuencës ose adresa IP janë të pandryshueshëm. SAODV përdor dy mekanizma për të siguruar mesazhet AODV: HMAC (KSD,M) përdoret për autentikimin e fushave të pandryshueshme të mesazhit të rrugëzimit M dhe një zinxhir çelësash HMAC për të siguruar numrin e hopeve. Funksioni HMAC merr një numër të ndryshueshëm argumentash thjesht duke i lidhur ato dhe llogarit kodin e autentikimit të mesazhit. Nyja burim përdor protokollin AODV për t'u lidhur me destinacionin. Kjo metodë siguron verifikim të shpejtë të mesazhit, autentikimin e mesazhit dhe të nyjeve të ndërmjetme.

3.6.9 Një protokoll eficient rrugëzimi bazuar në vendndodhjen anonime (ALERT)

ALERT e ndan rrjetin në zona dhe rastësisht zgjedh nyjet në zona si nyje të ndërmjetme pasuese, të cilat formojnë një rrugë anonime të pagjurmueshme. Në çdo hap rrugëzimi, një dërgues të dhënash ndan rrjetin në mënyrë që të ndajë veten dhe destinacionin në dy zona. Pastaj zgjedh rastësisht një nyje në zonën tjetër si nyjen tjetër pasuese dhe përdor algoritmin GPSR për të dërguar të dhënat në nyjen pasuese. [18] Në hapin e fundit, të dhënat dërgohen në zonën e destinacionit duke siguruar anonimitetin e destinacionit. Përveç kësaj, ALERT ka një strategji për të fshehur iniciatorin e të dhënave

mes disa iniciatorëve për të forcuar mbrojten e anonimitetit të burimit. Ky protokoll përdor ndarjen hierarkike dinamike të zonës dhe përzgjedhjen rastësore të nyjeve pasuese për të bërë të vështirë dedektimin e dy pikave fundore dhe nyjeve ne rrugë nga ndërhyrësit. Paketa në ALERT përfshin zonat e destinacionit dhe burimit në vend të pozicioneve të tyre për të siguruar mbrojtjen e anonimiteit të tyre. ALERT ka një zgjidhje efikase për sulmet e ndërprerjes së numërimit dhe sulmet timing.

3.6.10 Protokoll rrugëzimi i besueshëm bazuar në cluster (CBTRP)

Siguron rrugën e sigurtë dhe krijon mjedis të besuar. Ky mekanizëm përdoret për të përcaktuar nyjet e besueshme nga nyjet me qëllim të keq. CBTRP përdor protokollin WCA për zgjedhjen e cluster head-it [19]. Merren në konsideratë disa cilësi si fuqia e baterisë, numri i fqinjëve, fuqia e transmetimit dhe lëvizshmëria e nyjeve për të formuar CH-in optimal. Gjithashtu mer në konsideratë dhe sigurinë për të formuar cluster-a të besueshëm. Ai e organizon rrjetin në cluster-a me 1 hop ku çdo nyje është e aftë të zgjedhë nyjen më të kualifikuar dhe të besuar si CH i saj. Nyjet anëtare në cluster dërgojnë paketat nëpërmjet CH-ve të besueshëm. Nyjet me qëllim të keq nuk u dërgojnë paketa atyre. Në modelin CBTRP, vlera e besimit llogaritet duke u bazuar në informacionin që një nyje mund të mbledhë mbi informacionin jetësor të nyjeve të tjera përfshirë analizën e paketave të marra, të dërguara dhe të përgjuara. Analiza e sjelljes së nyjeve tregon që nyja është egoiste si black hole dhe mbart sulmin e modifikimit, fabrikimit dhe fshehjes së vonesave. Ky model siguron lidhje të përmirësuar në MANETs në prani të nyjeve me qëllim të keq dhe gjithashtu siguron kalimin e paketave nëpërmjet rrugëve të besueshme vetëm nga sjellja e çdo nyje. Kur zbulohet një nyje me qëllim të keq, ajo izolohet nga rrjeti, kështu që nuk dërgohet asnjë paketë nga ajo.

3.6.11 Protokoll rrugëzimi i bazuar në clustering i orientuar nga besueshmëria e sigurtë (STACRP)

Siguron një sistem të strukturuar të besueshëm për MANET. Përdor dy mekanizma ankand, të quajtur prokurim dhe Dutch për të përcaktuar koston e transmetimit të një hop-i. [21] Ky model e organizon rrjetin në cluster-a me 1 hop dhe zgjedh nyjet e besueshme si CH duke përdorur një skemë votimi sekret. Çdo nyje mban informacionin e vetes së saj dhe nyjeve fqinje për mirëmbajtjen e cluster-it. Modeli i besueshëm analizohet duke përdorur zinxhirin Markov i cili garanton revokimin e statusit të nyjes egoiste, nga status paralajmërimi në status normal nga dërgimi i duhur i paketave të tjera. Ky arrin një zgjidhje të sigurtë dhe të besueshme. STACRP dedekton nyjet egoiste dhe forcon bashkëpunimin ndërmjet nyjeve për të arritur performancë të mirë.

3.6.12 Siguria e algoritmit clustering bazuar në ngarkesë (SCA)

Zgjedh CH sipas ngarkesës së tyre të llogaritur duke kombinuar një sërë parametrash si stabiliteti, bateria, cilësia etj. [19] Për të krijuar ose mirëmbajtur arkitekturën clustering, fillimisht duhet të kryhet faza e zbulimit se cili informacion mbi fqinjësinë duhet të rigjendet. Për këtë qëllim, nyjet që duan të bëhen CH dërgojnë sinjalizimin CH_ready në rrezet me D hope rreth tyre. Pasi nyjet marrin sinjalizimin, vlerësojnë një vlerë besueshmërie dhe e dërgojnë mbrapsh. Pas një periode zbulimi, nyjet që kanë filluar këtë veprim, mund të përftojnë nga informacioni i përgjigjeve të marra, si cilësia, stabiliteti dhe vlera e besimit. Pastaj çdo nyje shton në parametrat e mëparshëm gjendjen e baterisë së saj, vlerën maksimale dhe i kombinon ato për të llogaritur ngarkesën e përgjithshme. Pasi nyjet zgjedhin CH i cili ka ngarkesën maksimale, çdo CH i sapo zgjedhur duhet të zbulojë të tjerët për të krijuar një shtyllë virtuale për komunikimin ndërmjet cluster-ve. Pra çdo CH i sapozgjedhur shpërndan një kërkesë zbulimi në rrjet. CH-të që e marrin këtë kërkesë regjistrojnë çertifikatën e CH të ri dhe dërgojnë çertifikatën e tyre.

3.6.13 Një cluster i sigurtë në MANET duke përdorur algoritmin Frd

Përfshin metodën FRD (niveli i lidhjes fuzzy) për procesin e zgjedhjes së CH, duke përfshirë disa parametra si jetëgjatësia, fuqia e baterisë, distanca ndërmjet tyre, shpejtësia e nyjeve dhe vlera FRD (μ) [20]. Çdo nyje në cluster duhet të ketë vlerën FRD të shënuar me μ. Kjo vlerë përdoret për të formuar një cluster të sigurtë me siguri të lartë dhe transferim optimal të paketave. Kjo vlerë μ përdoret nga nyjet në procesin e komunikimit i cili llogaritet duke përdorur parametrat si lëvizshmëria, distanca dhe fuqia. Skema e revokimit bëhet efektivisht nga nyja fqinje duke tejkaluar akuzën kundër nyjes korresponduese. Akuza e gabuar shmanget nga mirëmbajtja e VL (lista e votës) për të verifikuar statusin e nyjes akuzuese. Para procesit të revokimit krahasohet statusi i nyjes së akuzuar me VL. Prandaj probabiliteti i ndodhjes së akuzës së gabuar është shumë i vogël. Zgjedhja efiçente e CH dhe procesi i revokimit të çertificatës ndihmon në krijimin e një cluster-i të sigurtë dhe gjithashtu përmirëson performancën e rrjetit.

3.6.14 Algoritmi i zgjedhjes së CH bazuar në lidhjen Fuzzy (FRCA)

Përdoret në rrjeta me madhësi të ndryshueshme. FRCA ndan rrjetin në cluster-a dhe menaxhon në mënyrë efektive atë duke përdorur informacionin fuzzy të statusit të nyjes në rrjet. Ky algoritëm përdor nivelin e lidhjes fuzzy (FRD) me një vlerë fuzzy μ për të kryer dhe menaxhuar clustering [20]. Në këtë algoritëm FRD kryen clustering duke zgjedhur disa nyje që veprojnë si koordinatorë të clustering. Struktura e vëzhgimit të gjendjes fuzzy e cila kryen clustering konsiston në 5 parametra: ID, μ, Niveli, M-hop dhe ekuilibri. CH dhe anëtari i cluster-it zgjidhen duke përdorur vlerën fuzzy μ në strukturën e vëzhgimit të gjendjes fuzzy.

KAPITULLI 4

LOGJIKA FUZZY

4.1 Hyrje

Në literaturë gjenden justifikime të ndryshme për teorinë e sistemeve Fuzzy. Njohuritë njerëzore në ditët e sotme po bëhen gjithnjë e më të rëndësishme, ato i përfitojmë nga bota ku jetojmë dhe përdorim aftësitë tona për të arsyetuar për krijimin e një rregulli të informacionit. Pra jemi të kufizuar në aftësitë e perceptimit të botës dhe mund ta gjejmë veten kudo duke u përballur me pasiguri që vjen si rezultat i mungesës së informacionit. Një faktor tjetër i kufizimit në dëshirën për saktësi është gjuha e përdorur për përshkrimin apo shpërndarjen e informacionit, komunikimi etj. Ne kuptojmë kuptimet thelbësore të fjalës dhe mund të komunikojmë me saktësi në një nivel të pranueshëm, por në përgjithësi nuk mund të biem plotësisht dakort mes nesh në një fjalë të vetme apo sens të përbashkët.[39], [40]

Perceptimi i botës reale pushtohet nga koncepte që nuk kanë kufij të përcaktuar, psh. *shumë, i gjatë, më i madh se, i ri* etj. Janë të vërtetë në njëfarë mase dhe janë të gabuar në njëfarë mase tjetër. Këto koncepte mund të quhen Fuzzy ose të paqarta, truri i njeriut punon me to ndërsa kompjuteri nuk e bën këtë. Gjuhët natyrore janë Fuzzy ndërsa gjuhët e programimit nuk janë. Hapi i parë drejt zhvillimit të kompjuterave Fuzzy u bë nga Masakai Togai dhe Hiroyuki Watabane në 1985 me ndërtimin e një chip-i me logjikë Fuzzy.

Logjika Fuzzy u prezantua nga Lotfi Zadeh në vitin 1965 dhe është një mjet matematikor për të trajtuar pasiguritë. Ai i ofron informatikës konceptin e rëndësishëm të llogaritjes me fjalë si dhe siguron një teknikë që merret me pasaktësinë dhe "*granularity"* e informacionit. Teoria Fuzzy siguron një mekanizëm për paraqitjen e konstrukteve gjuhësore si *"shumë", "pak", "mesatar", "shpesh", "rrallë".*

Problemet e botës reale janë shumë komplekse, dhe kompleksiteti përfshin nivelin e pasigurisë. Teknikat e analizës dhe modelimit të sistemeve tradicionalë janë shumë të sakta për disa probleme (situata), dhe për ta bërë kompleksitetin më pak të frikshëm janë

futur thjeshtime të duhura, supozime etj, për të arritur një kompromis të kënaqshëm ndërmjet informacionit që kemi dhe vlerës së pasigurisë që jemi të gatshëm të pranojmë. Në këtë aspekt, teoria e sistemeve Fuzzy është e njëjtë me teoritë inxhinierike të tjera, sepse shumica prej tyre e karakterizojnë botën reale në një mënyrë të përafërt.

Në praktikë logjika fuzzy nënkupton llogaritjen me anë të fjalëve. Meqenëse llogaritja me fjalët është e mundur, sistemet e informatizuara mund të ndërtohen duke futur njohuritë njerëzore të artikuluara në gjuhën e përditshme. Sistemi Fuzzy i bazuar në rregulla ose Fuzzy inference mund të kryejë arsyetim të përafërt disi të ngjashëm por më primitive se truri i njeriut. Llogaritja me fjalë duket të jetë e ardhmja, duke qenë se aspekte të caktuara të gjuhës natyrore mund të paraqiten nga llogaritja e Fuzzy sets, dhe logjika Fuzzy mbetet një nga mënyrat më praktike të imitimit të njohurive njerëzore në një mënyrë realiste.

Modeli Fuzzy përdor një teknikë që njerëzit nuk përfaqësojnë klasat e objekteve plotësisht të ndara por si grupe në të cilët mund të ketë nivelet e anëtarësimit të ndërmjetme ndërmjet anëtarësimit të plotë dhe jo anëtarësimit. Termi “sistemet Fuzzy” i referehohen kryesisht sistemeve që rregullohen nga rregullat fuzzy “Në qoftë se .. – Atëherë …”. Një sistem Fuzzy është një set i rregullave fuzzy që konverton hyrjet në dalje. Sistemet Fuzzy nga njëra anë janë sisteme të bazuar në rregulla që ndërtohen nga rregullat gjuhësore, nga ana tjetër janë planifikim jolinear i hyrjeve tek daljet. Modelet Fuzzy nuk zëvendësojnë modelet probabilitare. Këto modele ndonjëherë funksionojnë më mirë dhe ndonjëherë jo. Por në të shumtën e rasteve Fuzzy siguron zgjidhje më të mira për problemet komplekse.

4.2 Kuptimi i Logjikës Fuzzy

Termi "Logjika fuzzy" (FL) përdoret aktualisht në dy kuptime të ndryshëm. Në një kuptim të ngushtë, FL është një sistem logjik që synon formalizimin e arsyetimit të përafërt. Si i tillë ai futet në sistemet e logjikës së vlerësimit.

Në një kuptim të gjerë, FL është e njëjtë me teorinë e Fuzzy set. Teoria e Fuzzy set, është në thelb një teori e klasave me kufij të paqartë dhe përfshin degë si: arithmetika

fuzzy, programimi matematikor fuzzy, topologjia fuzzy, teoria e grafit fuzzy dhe analiza e të dhënave fuzzy. Për të rritur aplikimin në botën reale mund të kalohet nga teoria klasike në teorinë e fuzzy set duke qenë se të dyja janë përgjithësim i teorisë. [39]

Në ditët e sotme po rritet tendenca e përdorimit të termit "logjika fuzzy" në kuptimin e gjerë të saj.

Logjika Fuzzy mund të përdoret sepse:

- Është konceptualisht e lehtë për t'u kuptuar. Konceptet matematikorë në arsyetimin Fuzzy janë të thjeshtë. Logjika Fuzzy është një metodë më intuitive dhe pa kompleksitet.
- Është fleksibile. Për një sistem të dhënë, është e lehtë të shtresëzohet në disa funksione pa filluar dhe njëherë nga e para.
- Është tolerante në të dhënat e pasakta. Në pamje të parë, por më shumë se kaq, shumë gjëra nuk janë të sakta madje dhe kur i shohim me kujdes. Logjika Fuzzy ndërton këtë kuptim në një proces në vend që ta marrë atë si përfundim.
- Mund të modelojë funksione jolinearë të kompleksitetit arbitrar. Mund të krijohet një sistem fuzzy për të përshtatur një set të dhënash hyrje-dalje.
- Ndryshe nga rrjetat neurale të cilët marrin të dhënat e formuara dhe gjenerojnë errësirë, modele të padepërtueshme, logjika fuzzy lejon mbështetjen në eksperiencën e njerëzve të cilët e kuptojnë sistemin.
- Mund të përzihet me teknikat konvencionale të kontrollit. Sistemet fuzzy nuk i zëvendësojnë këto teknika por i rrisin ato duke thjeshtuar implementimin e tyre.
- Bazohet në gjuhën natyrore. Baza për logjikën fuzzy është baza për komunikimin njerëzor.
- Meqenëse logjika fuzzy është ndërtuar mbi strukturat e përshkrimit cilësor të përdorura në gjuhën e përditshme është e lehtë për t'u përdorur.

4.2.1 Thelbi i logjikës fuzzy

Logjika fuzzy ka në thelb menyrat e arsyetimit të përafërt dhe jo të saktë. Rëndësia e saj vjen nga fakti që shumica e mënyrave të arsyetimit njerëzor janë kryesisht të përafërta. [41], [42]

Karakteristikat kryesore të logjikës fuzzy janë:

- Arsyetimi i saktë shihet si rast i kufizuar i arsyetimit të përafërt.
- Çdo gjë është çështje e nivelit.
- Sistemi logjik mund të fuzzified
- Njohuritë interpretohen si lidhje e kufizimeve fuzzy në një grup variablash.
- Inference shihet si një proces i përhapjes së kufizimeve elastike.

FL ndryshon nga sistemet tradicionalë logjikë në detaje. Ndryshimet kryesore jepen më poshtë:

- Vërtetësia

Në sistemet logjikë bivalent, vërtetësia mund të ketë dy vlera: e vërtetë ose e gabuar. Në sistemet e vlerësimit me shumë vlera, vlera e vërtetësisë për një problem mund të jetë një element i a) një set-i të fundëm, b) një intervali [0, 1], ose c) i algjebrës booleane. Në FL, vlera e vërtetë e një problemi mund të jetë një subset fuzzy në intervalin [0, 1] ose një pikë në këtë interval. Vlerat gjuhësore të vërtetësisë të shprehura si i saktë, shumë i saktë, ose jo plotësisht i saktë interpretohen si emërtime të subset-ve fuzzy në intervalin njësi.

- Pohimet

Në sistemet bivalente, pohimet janë të mirë përcaktuara (crisp). Në FL, pohimet janë fuzzy, psh. *i gjatë, i vjetër, më i gjatë se* etj. Në fakt shumica e pohimeve në gjuhën natyrore janë fuzzy dhe jo crisp.

- Modifikuesit e pohimeve

Në sistemet klasike, modifikuesi më i përdorshëm i pohimeve është mohimi nuk. Në FL, ka disa modifikues të pohimeve që veprojnë si pengesa, psh. *Shumë, shumë ose pak, i qetë, më tepër, jashtëzakonisht*. Disa modifikues luajnë një rol të rëndësishëm në gjenerimin e vlerave të variablave gjuhësorë, psh. *shumë i ri, jo shumë i ri, më i ri ose më pak i ri*.

- Kuantifikuesit

Në sistemet logjikë ka vetëm dy kuantifikues: universal dhe egzistencial. FL pranon një shumëllojshmëri kuantifikuesish fuzzy të ilustruar nga *pak, disa, shumica, pothuajse, gjithmonë, rreth pesë,* etj. Në FL, një kuantifikues fuzzy interpretohet si një numër fuzzy ose proporcion fuzzy.

- Probabilitetet

Në sistemet klasikë logjikë, probabiliteti është numër ose interval vlerash. FL ka opsionin shtesë të përdorimit të mundësive gjuhësore ose më në përgjithësi probabilitetet fuzzy si *e pritshme, e papritur, shumë e pritshme, rreth 0.8,* etj. Probabilitete të tilla mund të interpretohen si numra fuzzy që mund të manipulohen me përdorimin e aritmetikës fuzzy.

- Mundësitë

Ndryshe nga logjika klasike, koncepti i mundësive në FL vlerësohet më tepër se bivalent. Në rastin e probabiliteteve, mundësitë mund të trajtohen si variabla gjuhësorë me vlera të tilla si *e mundur, krejt e mundur, pothuajse, e pamundur*, etj.Vlera të tilla mund të interpretohen si shifra të subset-ve fuzzy në realitet. Është e rëndësishme të vihet re se në çdo rast FL shton mundësitë të cilat janë në dispozicion në sistemet klasike logjike. Në këtë kontekst, FL mund të shihet si një zgjerim i sistemeve të tilla dhe jo si një sistem i arsyetimit që është në kundërshtim me sistemet klasike.

4.3 Bazat e teorisë së Fuzzy set

Koncepti i një set fuzzy lidhet me përfaqësimin e klasave të cilave nuk ju dihet kufiri. Ajo përdor një funksion karakteristik që merr zakonisht vlerat në intervalin [0, 1]. Fuzzy sets përdoren për paraqitjen e emërtimeve gjuhësore. Fuzzy sets dhe logjika fuzzy janë krijuar për të menaxhuar paqartësinë dhe pasigurinë në një proces arsyetues të një sistemi inteligjent siç janë sistemet e bazuara në njohuri, sistemet eksperte ose sistemet llogjike të kontrollit. [43]

Teoria e fuzzy set përdor funksionin e anëtarësimit për të shifruar një preferencë mes interpretimeve të mundshme të emërtimit përkatës. Një set fuzzy mund të përcaktohet

nga ilustrimi, renditja e elementëve sipas tipit të tyre në lidhje me konceptin themelor të fuzzy set.

Elementi prototip merr vlerën më të madhe të anëtarësimit. Në çdo rast fuzzy sets ruajnë një kalim gradual dhe të qetë nga një kategori në tjetrën dhe shmangin ndërprerjet e menjëhershme që mund të shkaktohen nga caktimi i kufijve të saktë për subset të caktuar. Në këtë rast, fuzzy sets sigurojnë një mjet për tejkalimin e hendekut ndërmjet vazhdimësisë së perceptuar të botës dhe përfaqësimit njohës diskret njerëzor. Veçanërisht, fuzzy sets ndihmojnë me ndërfaqen e të dhënave numerike dhe emërtimeve simbolike.

4.3.1 Kuantifikimi i paqartësisë

Shumica e gjuhëve natyrore përmbajnë paqartësi dhe shumëllojshmërinë e kuptimit. Veçanërisht objektet e mbiemrave nuk janë specifikuar në mënyrë të qartë, dhe janë të paqarta sa i përket kuptimit. Nqs themi "*njeri i gjatë*", nuk e përcaktojmë saktësisht kush është i gjatë dhe kush nuk është i gjatë. [43] Fjalët në përgjithësi janë kualitative, por disa si "i gjatë" dhe "i vjetër" perceptohen në lidhje me vlerat e gjatësisë ose moshës.Veçanërisht në inxhinieri, mbiemrat që përshkruajnë gjendjen dhe kushtet e gjërave të ndryshme janë të lidhur pothuajse gjithmonë me sasitë. Le të shohim paqartësinë e kuptimit "*i gjatë*" në aspektin e shprehjes së shumës. Në rendin e gjatësisë nga 140 në 200 cm, niveli i tillë që x[cm] mund të quhet i gjatë është μ, pra bëjmë gjatësinë x t'i korrespondojë nivelit $\mu\,(0 \le \mu \le 1)$. Në qoftë se boshti horizontal është x dhe boshti vertikal është μ, grafiku do ishte si në figurën 4.1.

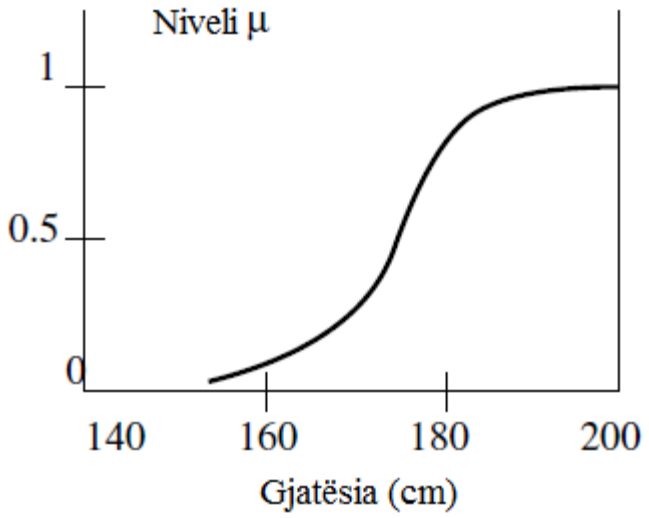


Figura 4.1. Niveli i “i gjatë”

Ky grafik shpreh paqartësinë e “i gjatë” në aspektin e sasisë. Boshti horizontal është kuantifikimi i fjalës, shprehja e gjatësisë në hapësirën një dimensionale, dhe boshti vertikal është kuantifikimi i nivelit të paqartësisë. Kjo mënyrë shprehjeje e fjalës quhet kuantifikim i kuptimit. Kuptimi i fjalës kuantizohet në një rend të caktuar, për gjatësinë ky rend është 140 cm deri 200 cm.

4.3.2 Përkufizimet e fuzzy set

Një fuzzy set është një klasë me kufij të paqartë, në të cilën kalimi nga anëtarësim në mos-anëtarësim është gradual dhe jo i menjëhershëm. Seti përfshin objektet që kanë një ose më shumë karakteristika të njëjta. [44] Anëtari përfshin objektet që i përkasin një seti.

Më poshtë jepen disa nocione themelore për futjen e teorisë së fuzzy set.

- X – gjithë set-i
- E – subset i X
- ϕ - set bosh
- {0, 1} – set i zero dhe 1

- [0, 1] – interval i numrave realë nga 0 në 1
- χ_E - funksioni karakteristik i set E
- $a \wedge b$ - minimum i a dhe b
- $a \vee b$ - maksimumi i a dhe b

Një fuzzy set është zgjerim i një crisp set. Crisp set lejojnë vetëm anëtarësimin e plotë ose jo anëtarësimin, ndërsa fuzzy sets lejojnë anëtarësimin e pjesshëm. Pra një element mund t'i përkasë pjesërisht një set-i. Në një set crisp, anëtarësimi ose jo anëtarësimi i një elementi x në set E, ku E është subset i X, përshkruhet me ekuacionin karakteristik të mëposhtëm:

$$\chi_E = \begin{cases} 1; x \in E \\ 0; x \notin E \end{cases} \tag{4.1}$$

Ky i korrespondon funksionit të anëtarësimit të E. Niveli ka dy vlera; nqs x përfshihet në E është 1 dhe nqs jo është 0. Nga ana tjetër një fuzzy set është një klasë me kufij fuzzy.
Një paraqitje abstrakte e një fuzzy subset i X set ka pamjen si në figurën 4.2.

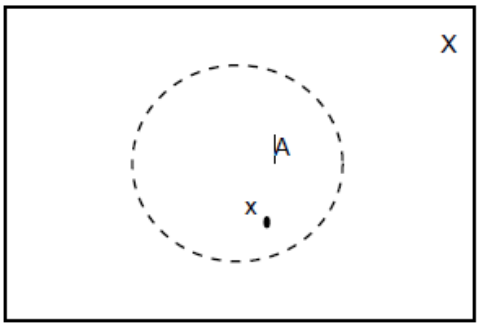


Figura 4.2. Fuzzy subset A

Forma drejtkëndësh tregon set X, rrethi me vija të ndërprera tregon subset të X që përcaktohet nga A. Teoria e fuzzy set përcakton nivelin në të cilin elementi x i set X përfshihet në këtë subset. Funksioni që jep nivelin në të cilin ai përfshihet quhet funksioni i anëtarësimit.
Përkufizimi i plotë i fuzzy set jepet nga përcaktimet e mëposhtme.

Përcaktimi 1

Le të jetë X={x} universi (grupi i objekteve), i përcaktuar në përgjithësi nga x; atëhere një subset fuzzy i X, A, është një set i çifteve të caktuara $(x, \mu_A(x)), x \in X$, ku $\mu_A(x)$ është niveli i anëtarësimit të x në A, dhe $\mu_A: X \to [0,1]$ është funksioni i anëtarësimit.

Meqenëse një fuzzy set përcaktohet gjithmonë si subset i një set të përgjithshëm X, "sub" është shkurtim i vazhdueshëm, dhe thjesht quhet një fuzzy set.

Nga përcaktimi shohim që funksioni gjatë intervalit [0, 1] ka një korrespondencë me fuzzy set. Ky funksion është një kuantifikim i paqartësisë apo dykuptimësisë (ambiguity) të zones A. Në fakt, ky funksion ka të njëjtat karakteristika si në figurën 4.1 e cila mund të mendohet si një përfaqësim i funksioneve të anëtarësimit të fuzzy set "grupi i gjatësive që mund të mendohen si të gjatë" brenda grupit të gjatësive nga 140 cm deri 200 cm.

Megjithatë, ka shumë fuzzy set dhe çdo formë e funksioneve të anëtarësimit është e mundur, ndaj fuzy sets nuk korrespondojnë gjithmonë me fjalët. Nqs mendojmë për funksionin e anëtarësimit jo vetëm për "i gjatë", por gjithashtu për "rreth mesatar" dhe "i shkurtër", funksioni i anëtarësimit do ketë pamjen si në figurën 4.3. Siç shihet nga figura, ka dy gjëra bazë të kontrollit fuzzy set. I pari është boshti horizontal që është gjithë set X. X quhet set mbeshtetës i fuzzy set ose thjesht suport. I dyti është funksioni i anëtarësimit. Çdokush mund të mendojë që funksioni i anëtarësimit të "rreth mesatar" qëndron në mes, por niveli nga 150 deri 170 cm mund të ndryshojë subjektivisht me personin që po mendon. Në këtë mënyrë, fuzzy set mund të shihen si subjektivë, ndryshe me set standart të cilët janë objektivë.

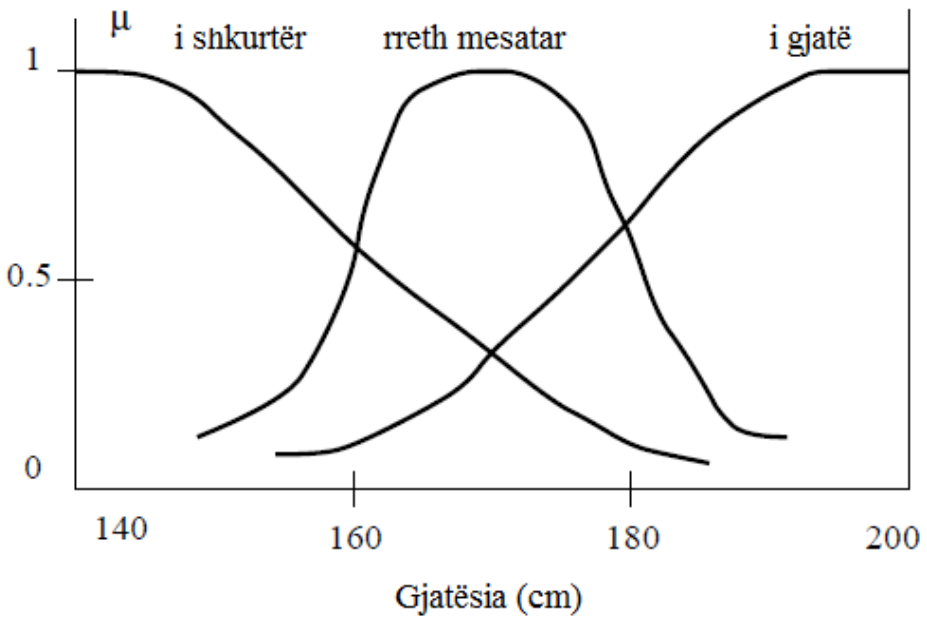


Figura 4.3. Funksioni i anëtarësimit për "i shkurtër", "rreth mesatar", "i gjatë"

Më poshtë jepen disa përkufizime për veprimet me fuzzy sets.

Përcaktimi 2

Barazia. Nqs A dhe B janë fuzzy subsets të X, atëhere A dhe B janë të barabarta, dhe shënohet A=B, vetëm nqs $\mu_A(x) = \mu_B(x), \forall x \in X$ (4.2)

Përcaktimi 3

Përfshirja. Nqs A dhe B janë fuzzy subsets të X, atëhere A është subset i B, shënohet $A \subseteq B$ nqs dhe vetëm nqs: $\mu_A(x) \leq \mu_B(x), \forall x \in X$ (4.3)

Përcaktimi 4.

Komplementi. Komplementi i një fuzzy subset të X shënohet $\overline{A}$, përcaktohet si më poshtë: $\mu_{\overline{A}}(x) = 1 - \mu_A(x), \forall x \in X$ (4.4)

Përcaktimi 5.

Bashkimi. Bashkimi i dy fuzzy subsets, A dhe B të X, shënohet si $A \cup B$, përcaktohet nga:

$$\mu_{A\cup B}(x) = \max(\mu_A(x), \mu_B(x), \forall x \in X \tag{4.5}$$

Përcaktimi 6.

Ndërprerja. Ndërprerja e dy fuzzy subsets A dhe B të X, shënohet si $A \cap B$, përcaktohet si:

$$\mu_{A\cap B}(x) = \min(\mu_A(x), \mu_B(x), \forall x \in X \tag{4.6}$$

Përcaktimi 7.

Përqendrimi. Përqendrimi i një fuzzy set A të X, shënohet $\mu_{CON(A)}(x)$, përcaktohet nga:

$$\mu_{CON(A)}(x) = \mu_A{}^2(x), \forall x \in X \tag{4.7}$$

Përcaktimi 8.

Hollimi. Hollimi i një fuzzy subset A të X, shënohet $\mu_{DIL(A)}(x)$, përcaktohet nga:

$$\mu_{DIL(A)}(x) = \sqrt{\mu_A(x)}, \forall x \in X \tag{4.8}$$

Përcaktimi 9.

Lidhjet Fuzzy. Le të jenë X={[x]} dhe Y={[y]}dy fusha arbitrare të universit. Lidhja fuzzy R nga X te Y është një fuzzy subset i produktit kartezian XxY={[x,y]}, që karakterizohet nga funksioni i anëtarësimit $\mu_R : X \times Y \to [0,1]$ i cili shoqëron çdo çift {x,y}me nivelin e anëtarësimit $\mu_R(x, y)$ në R.

Përcaktimi 10.

Kompozimi Fuzzy. Le të jetë R një lidhje fuzzy në $X \times Y$ dhe S një lidhje fuzzy në $Y \times Z$. Kompozimi i R dhe S, $R \circ S$, është një lidhje fuzzy në $X \times Z$ që përcaktohet nga:

$$R \circ S \leftrightarrow \mu_{R\circ S}(x, z) = \vee_y \{(\mu_R(x, y) \wedge \mu_S(y, z))\}, \tag{4.9}$$

ku $\vee = \max$, $\wedge = \min$.

Ky kompozim përdor veprimet max dhe min, ndaj quhet kompozimi max-min.

4.3.3 Variablat gjuhësorë

Variablat gjuhësorë luajnë një rol të rëndësishëm në aplikimin e FL. Konsiderojmë funksionet e anëtarësimit të figurës 4.3. Variabli gjuhësor është "*gjatësia*" vlerat gjuhësore të të cilit janë i *shkurtër, mesatar, i gjatë*. *I gjatë* përcaktohet nga funksioni i

anëtarësimit si në figurën 4.1. Një vlerë numerike si 170 është më e thjeshtë se funksioni *i gjatë*. Por *i gjatë* paraqet një zgjedhje të një prej tre vlerave të mundshme ku 170 është një zgjedhje të njërës nga, le të themi, 200 vlerave. Qëllimi i këtij shembulli është që variablat gjuhësorë mund të shihen si formë e kompresimit të të dhënave. Sugjerohet t'i referohemi këtij kompresimi të dhënash si kokrrizim (granulation). I njëjti efekt mund të arrihet nga kuantizimi konvencional, por në rastin e kuantizimit, vlerat janë interval, ndërsa në rastin e kokrrizimit vlerat janë fuzzy set të mbivendosur. Avantazhet e kokrrizimit ndaj kuantizimit janë si më poshtë:

- Është më i përgjithshëm
- Imiton mënyrën me të cilën njerëzit interpretojnë vlerat gjuhësore
- Kalimi nga një vlerë gjuhësore në një vlerë të afërt gjuhësore është gradual dhe jo i papritur, duke rezultuar në vazhdimësi dhe forcë.

4.4 Kontrolli Fuzzy

Aftësia e fuzzy sets dhe mundësitë teorike të modelimit gradual të karakteristikave apo kufizimet e lehta, plotësimi i të cilave matet me nivele, si dhe informacioni i mbushur me pasaktësi dhe paqartësi, e bëjnë logjikën fuzzy të nevojshëm në aplikime të ndryshme. Fusha më e përhapur e aplikimit është kontrolli fuzzy (FC), në industri, kontroll procesi, sistemet automobilistikë dhe shumë fusha të tjera. Në sistemet FC, njohuritë e ekspertëve janë të koduar në formën e rregullave fuzzy, të cilat përshkruajnë veprimet e rekomanduara për tipe të ndryshme të situatave të përfaqësuara nga fuzzy sets. Metodologjia FC siguron një mekanizëm interpolimi. [45]

Situatat aktuale që hasen nga sistemi ngjajnë pjesërisht me dy ose më shumë situata prototip për të cilat veprimet e kontrollit të rekomanduara njihen, dhe një veprim kontrolli që është ndërmjetës ndërmjet këtyre rekomandimeve llogaritet në bazë të nivelit të ngjashmërisë. Një njësi FC mund të bëjë të njëjtën punë si një kontroller PID, pasi ajo në mënyrë implicite përcakton një funksion numerik që lidh së bashku variablat e kontrollit dhe ndryshoret e vërejtura të kontrollit. Ndryshimi ndërmjet metodave klasike dhe FC qëndron në mënyrën se si gjendet ligji i kontrollit. Në kontekstin e kontrollit automatik

klasik, sidomos teoria e kontrollit optimal, ligji i kontrollit llogaritet duke përdorur një model matematik të procesit, ndërsa modeli FL, në përputhje me inteligjencën artificiale, sugjeron që ligji i kontrollit të ndërtohet duke filluar nga ekspertiza e një operatori njerëzor. Në aplikimet e kontrollerave PID, filozofia është pranë kontrollerit FL, duke qenë se akordimi i parametrave PID bëhet zakonisht në një mënyrë ad hoc.

Megjithatë, vetëm ligjet linearë mund të arrihen me një PID, ndërsa kontrolleri fuzzy mund të kapë ligjet jo-linearë që shpjegojnë dhe suksesin e kontrollerave fuzzy ndaj atyre PID. Në fakt një ligj kontrolli mund të modelohet me metodologjinë FC, me kusht që ky ligj është i shprehshëm në termat e rregullave "Në qoftë se.. Atëherë..", si në rastin e sistemeve eksperte. Megjithatë FL ndryshon nga sistemi ekspert standart duke siguruar një mekanizëm interpolimi nga disa rregulla.

Në kontekstin e proceseve kompleksë, ai mund të jetë më praktik për të marrë njohuritë nga një operator ekspert sesa të llogarisë një kontroll optimal, për shkak të kostos së modelimit apo sepse modeli është i paarritshëm.

4.4.1 Kontrolleri Fuzzy logic (FLC)

Shumica e produkteve komerciale të kontrollerave fuzzy janë sisteme të bazuar në rregulla të cilët marrin informacionin aktual nga reagimi i pajisjes që ajo vepron dhe kontrollon veprimin e një pajisje mekanike ose pajisje të tjera. [45], [46] Sistemi i logjikës fuzzy ka katër blloqe si në figurë. Informacioni i hyrjes crisp nga pajisja konvertohet në vlera fuzzy për çdo hyrje të grupit fuzzy në bllokun e fuzzification. Universi i variablave hyrës përcakton shkallëzimin e kërkuar për veprimin e saktë për njësi. Shkallëzimi është shumë i rëndësishëm sepse sistemi fuzzy mund të përzihet me pajisje të tjera ose rende të veprimit duke ndryshuar shkallëzimin për hyrjen dhe daljen. Logjika e marrjes së vendimeve përcakton sesi kryhen veprimet e logjikës fuzzy dhe bashkë me bazën e njohurive përcakton daljet për çdo rregull fuzzy "Në qoftë se - Atëherë…". Këto kombinohen dhe konvertohen në vlera crisp në bllokun e defuzzification. Vlera e daljes crisp mund të llogaritet me qendrën e gravitetit ose mesataren e ponderuar.

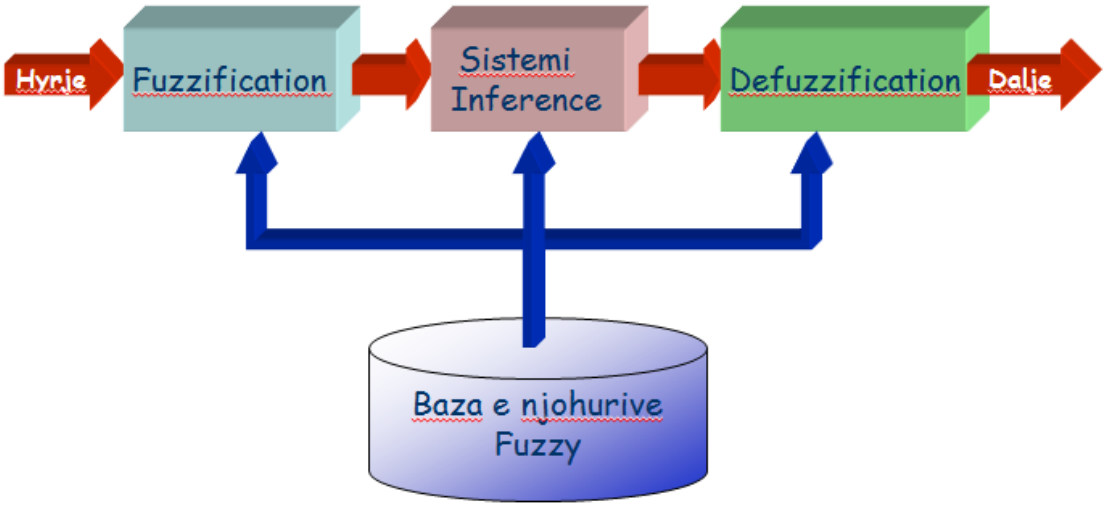


Figura 4.4. Diagrama bllok e FLC

Në krijimin e sistemit fuzzy të bazuar në rregulla përfshihen gjashtë hapa:

1. Identifikimi i hyrjeve, rendet dhe emërtimi i tyre.
2. Identifikimi i daljeve, rendet dhe emërtimi i tyre.
3. Krijimi i nivelit të funksionit të anëtarësimit fuzzy për çdo hyrje dhe dalje.
4. Ndërtimi i bazës së rregullit sipas të cilit do veprojë sistemi.
5. Vendimi si do egzekutohet veprimi duke caktuar karakteristikat e rregullave.
6. Kombinimi i rregullave dhe defuzzification i daljes.

4.5 Fuzzification

Fuzzification është një koncept i rëndësishëm i teorisë së fuzzy logic. Fuzzification është procesi ku një set crisp konvertohet në fuzzy. Vlerat fuzzy formohen duke identifikuar disa pasiguri prezente në vlerat crisp. [48] Konvertimi i vlerave fuzzy paraqitet nga funksionet e anëtarësimit. Në aplikimet reale si industri, matja e tensionit, rrymës, temperaturës etj. mund të ketë gabime të papërfillshme. Kjo shkakton pasaktësi në të dhëna. Kjo pasaktësi mund të përfaqësohet nga funksionet e anëtarësimit. Kështu

kryhet fuzzification. Pra procesi i fuzzification përfshin përcaktimin e vlerave të anëtarësimit për sasi të dhëna crisp.

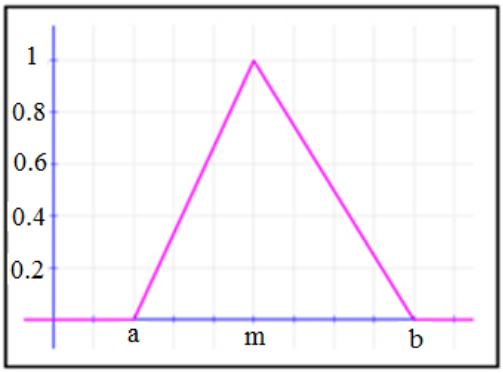
4.5.1 Funksionet e anëtarësimit

Funksioni i anëtarësimit për një fuzzy set A në universin X përcaktohet si: $\mu_A : X \rightarrow [0,1]$ ku çdo element i X planifikohet në një vlerë ndërmjet 0 dhe 1. [45] Kjo vlerë quhet vlera e anëtarësimit ose niveli i anëtarësimit, vlerëson nivelin e anëtarësimit të elementit në X të fuzzy set A.

Funksionet e anëtarësimit lejojnë paraqitjen grafike të një fuzzy set. Boshti x paraqet universin, ndërsa boshti y paraqet nivelin e anëtarësimit në intervalin [0,1].

Më poshtë jepen disa tipe të funksioneve të anëtarësimit.

1. Funksioni trekëndor, përcaktohet nga një vlerë kufi më të ulët a, një kufi të sipërm b, dhe një vlerë m, ku a <m <b, si në figurën 4.5.a.

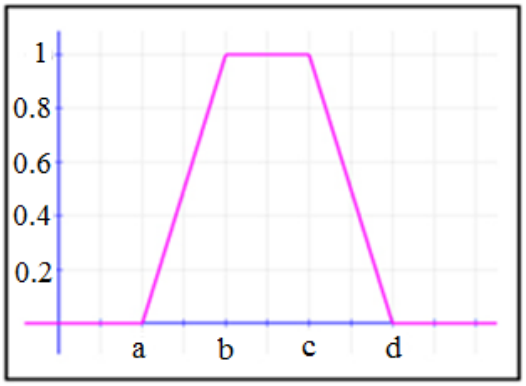


4.5.a. Funksioni trekëndor

$$\mu_A(x) = \begin{cases} 0, \rightarrow x \leq a \\ \dfrac{x-a}{m-a}, \rightarrow a < x \leq m \\ \dfrac{b-x}{b-m}, \rightarrow m < x < b \\ 0, \rightarrow x \geq b \end{cases}$$

$$\text{Ose } \mu_A(x) = \max(\min(\frac{x-a}{m-a}, 1, \frac{b-x}{b-m})) \tag{4.10}$$

2. Funksioni trapezoidal: përcaktohet nga një kufiri i poshtëm a, kufiri i sipërm d, kufiri i sipërm mbështetës c, dhe kufiri i poshtëm mbështetës b, ku a <b <c <d, si në figurën 4.5.b

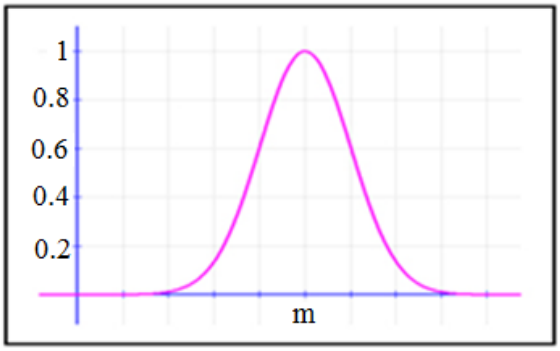


4.5.b. Funksioni trapezoidal

$$\mu_A(x) = \begin{cases} 0, \rightarrow x < a \\ \frac{x-a}{b-a}, \rightarrow a \le x \le b \\ 1, \rightarrow m \le x \le c \\ \frac{d-x}{d-c}, \rightarrow c \le x \le b \end{cases}$$

$$\text{Ose } \mu_A(x) = \max(\min(\frac{x-a}{b-a}, 1, \frac{d-x}{d-c})) \tag{4.11}$$

3. Funksioni Gausian, përcaktohet nga një vlerë qendrore m dhe një devijim standart k>0. Sa më e vogël është k aq më e ngushtë është "këmbana", si në figurën 4.5.c.



4.5.c. Funksioni gausian

$$\mu_A(x) = e - \frac{(x-m)^2}{2k^2} \tag{4.12}$$

Figura 4.5. Funksioni i anëtarësimit

Fuzziness në një fuzzy set karakterizohet nga funksionet e tij të anëtarësimit. Ai i klasifikon elementet në set, qoftë diskret ose i vijueshëm. Funksionet e anëtarësimit mund të formohen gjithashtu nga paraqitje grafike e cila mund të përfshijë forma të ndryshme. Forma e funksionit të anëtarësimit është një kriter i rëndësishëm që duhet marrë në konsideratë. Ka metoda të ndryshme për të formuar funksionet e anëtarësimit. Në sistemet e propozuar bazohemi në intuitë për përcaktimin e funksioneve të anëtarësimit.

4.5.2 Karakteristikat e Funksionit të Anëtarësimit

Karakteristikat e Funksionit të Anëtarësimit përcaktohen nga tre veçori:

1. Pjesa qendrore, Nëse zona e universit karakterizohet me anëtarësim të plotë (1) në setin $\underline{A}$ atëherë kjo jep pjesën qendrore të funksionit të anëtarësimit. Elementët që kanë funksionin e anëtarësimit 1, janë elementët e pjesës qendrore $\mu \underline{A}(x) = 1$

2. Mbështetja, Nëse zona e universit karakterizohet nga anëtarësimi jo zero në set-in $\underline{A}$, kjo përcakton mbështetjen e një funksioni të anëtarësimit për fuzzy set $\underline{A}$. Mbështetja ka elementë anëtarësimi i të cilëve është më i madh se 0. $\mu \underline{A}(x) > 0$.
3. Kufiri, Nëse zona e universit ka një anëtarësim jo zero por jo të plotë, kjo përcakton kufirin e një funksion anëtarësimi për një fuzzy set $\underline{A}$. Kufiri ka elementët funksioni i anëtarësimit të të cilëve është ndërmjet 0 dhe 1, $0 < \mu \underline{A}(x) < 1$.

Përcaktohen dhe dy terma të rëndësishëm:

Pika crossover e një funksioni anëtarësimi janë elementet në univers vlera e anëtarësimit të të cilëve eshte i barabartë me 0.5, $\mu \underline{A}(x) = 0.5$

Lartësia e një fuzzy set $\underline{A}$ është vlera maksimale e funksionit të anëtarësimit, $\max(\mu \underline{A}(x))$

Funksioni i anëtarësimit mund të jetë simetrik ose asimetrik.

4.5.3 Përcaktimi i vlerës së anëtarësimit

Ka metoda të ndryshme për përcaktimin e vlerave të anëtarësimit. Përcaktimi mund të bëhet me intuitë ose duke përdorur algoritme ose procedura logjike. [43], [45] Disa metoda të përcaktimit të vlerave të anëtarësimit janë:

Intuita, bazohet në inteligjencën njerëzore dhe të kuptuarit për të zhvilluar funksionet e anëtarësimit. Duhet të njihen problemi dhe variablat gjuhësorë.

Inference, përfshin njohuritë për të kryer arsyetimin deduktiv. Funksioni anëtarësimit formohet nga faktet e njohura dhe njohuritë.

Radhitja, Këtu përdoret koncepti i votimit për të caktuar vlerat e anëtarësisë me procesin e rradhitjes. Formimi i rradhitjes i anëtarësimit kryhet duke u bazuar në karahasimet e preferencave.

Rrjetat neurale, përdoren për të simuluar rrjetin e punës së neuroneve në trurin e njeriut. Koncepti i trurit njerëzor përdoret për të kryer llogaritje në kompjuter.

Algoritme gjenetike (GA), përdorin konceptin e teorisë së evolucionit të Darwinit. Teoria e Darwinit bazohet në rregullin, "mbijetesa e më të fortit."

Arsyetimi induktiv, anëtarësimi mund të gjenerohet nga karakteristikat e arsyetimit induktiv. Induksioni kryhet nga principi i minimizimit të entropisë, i cili grumbullon parametrat që i korrespondojnë klasave të daljes. Duhet të ketë një bazë të dhënash të mirë përcaktuar për të kryer këtë metodë.

4.6 Defuzzification

Përfundimi ose dalja e kontrollit që rrjedh nga kombinimi i hyrjes, funksioneve të anëtarësimit të daljes dhe rregullat fuzzy është e paqartë ose element fuzzy, dhe ky proces quhet inference fuzzy.[50] Për ta bërë këtë dalje fuzzy të përshtatshme për aplikimet reale nevojitet procesi i defuzzification. Defuzzification ka si qëllim konvertimin e daljes fuzzy në dalje crisp ose klasike të objektivit të kontrollit. Kujtojmë që dalja fuzzy është variabël gjuhësor i cili duhet të konvertohet në vlerë crisp nëpërmjet procesit të defuzzification.

Në literaturë gjenden metoda të ndryshme defuzzification. Mes tyre, katër janë metodat që janë aplikuar më shumë.

4.6.1 Metoda e defuzzification Tsukamoto

Nqs përdoren funksionet e anëtarësimit *monotonic*, atëhere një veprim kontrolli crisp mund të llogaritet me: $Z^* = \frac{\sum_{i=1}^{n} \omega_i x_i}{\sum_{i=1}^{n} \omega_i}$ (4.13)

Ku n është numri i rregullave me forcë ndezje (ω_i) më të madhe se 0 dhe x_i është vlera e veprimit të kontrollit të rekomanduar nga rregulli i.

4.6.2 Metoda e qendrës së zonës (COA)

Kjo metodë është teknika e defuzzification më e përdorur në aplikime aktuale. Eshtë e ngjashme me formulën e llogaritjes së qendrës së gravitetit në fizikë. Qendra e

gravitetit të zonës e kufizuar nga kurba e funksionit të anëtarësimit llogaritet të jetë vlera më e mirë-përcaktuar e sasisë fuzzy.

Supozojmë që përftohet një veprim kontrolli me funksion anëtarësimi pointwise μ_C. Metoda COA llogarit qendrën e gravitetit të shpërndarjes për veprimin e kontrollit. Për një univers diskret kemi: $Z^* = \frac{\sum_{j=1}^{q} z_j \mu_C(z_j)}{\sum_{j=1}^{q} \mu_C(z_j)}$ (4.14)

Ku q është numri i niveleve të kuantizimit të daljes, z_j është vlera e daljes së kontrollit në nivelin e kuantizimit j dhe $\mu_C(z_j)$ paraqet vlerën e funksionit të anëtarësimit të tij në C.

4.6.3 Metoda e mesit të maksimumit (MOM)

Kjo metodë llogarit mesataren e daljeve fuzzy që kanë nivelet më të larta.

Kjo metodë gjeneron një veprim kontrolli crisp duke mesatarizuar vlerat e suportit vlerat e anëtarësimit të të cilave arrijnë maksimumin. Për një univers diskret, kjo llogaritet:

$$Z^* = \sum_{i=1}^{l} \frac{z_j}{l} \tag{4.15}$$

Ku l është numri i vlerave të kuantizuara z të cilat arrijnë maksimumin e tyre të anëtarësimeve.

Një e metë e metodës MOM është që nuk konsideron të gjithë formën e funksionit të anëtarësimit të daljes, por mer parasysh pikat që kanë nivelet më të larta në këtë funksion. Pra, për forma të ndryshme të FA por që kanë të njëjtat nivele maksimale, kjo metodë nxjerr të njëjtin rezultat.

4.6.4 Defuzzification ku dalja e rregullave është funksion i hyrjes.

Rregullat FC mund të shkruhen si një funksion i hyrjeve të tij. Për shembull,

Rregulli i: Nqs X është A_i dhe Y është B_i atëhere Z është $f_i(X,Y)$;

Marrim që α_i është forca e ndezjes së rregullit i, atëhere: $Z^* = \frac{\sum_{i=1}^{n} \alpha_i f_i(x_i, y_i)}{\sum_{j=1}^{n} \alpha_i}$ (4.16)

4.7 Sistemi Fuzzy i bazuar në rregulla

Rregullat formojnë bazën për logjikën fuzzy për të marrë daljen fuzzy. Sistemi i bazuar në rregulla ndryshon nga sistemi ekspert në mënyrën që rregullat e përfshira në sistemin e bazuar në rregulla rrjedhin nga burime të tjera dhe jo njerëzore, prandaj ndryshojnë nga sistemet njerëzore. [46] Sistemi i bazuar në rregulla përdor variablat gjuhësorë si shkaqe dhe pasoja. Shkaqet shprehin një konkluzion ose pabarazi që duhet të kënaqet. Pasojat janë ato të cilat mund të konkludohen, dhe është përfundimi ose dalja nqs pasoja është kënaqur. Sistemi fuzzy i bazuar në rregulla përdor logjikën " Në qoftë se… - Atëherë…", të dhënë nga "Në qoftë se" është shkaku dhe "Atëherë" është pasoja.

4.7.1 Formimi i rregullave

Formimi i rregullave në përgjithësi është kanonik.

Për variablin gjuhësor ka tre forma kryesore të formimit të rregullave kanonike.[45]

1.Formulime të caktimit. Këto formulime janë ato në të cilat variabli caktohet me një vlerë. Variabli dhe vlera e caktuar kombinohen nga operatori i caktimit "=". Këto formulime janë të domosdoshme në formimin e rregullave. Vlera që caktohet mund të jetë një term gjuhësor. Psh. Qielli = blu; a=5 etj.

2.Fomulime të kushtëzuara. Në këto formulime theksohen disa kushte specifike, dhe në qoftë se kushtet kënaqen atëhere ato futen në formulimet në vijim dhe quhen kufizime. Psh Nqs x=y atëhere ato janë të njëjta.

3.Formulime të pakushtëzuara. Këtu nuk ka ndonjë kusht të caktuar që duhet të kënaqet. Psh. Fut vlerën, Stop etj.

4.7.2 Sistemi i inference fuzzy (FIS)

Këto sisteme njihen dhe si sisteme fuzzy të bazuar në rregulla, model fuzzy, sistem ekspert fuzzy. Kjo është njësia kryesore e një sistemi logjik fuzzy. Marrja e vendimeve është një pjesë e rëndësishme e gjithë sistemit. [45], [49] Sistemi i inference fuzzy formulon rregulla të përshtatshme dhe në bazë të rregullave merret vendimi. Kjo bazohet kryesisht në konceptet e teorisë fuzzy set, rregullat fuzzy "Në qoftë se.. – Atëherë.." dhe arsyetimi fuzzy. FIS përdor formulimet "Në qoftë se.. – Atëherë…", dhe lidhësit "OR"ose "AND" për të formuluar rregullat e duhura. FIS bazë mund të marrë hyrjet fuzzy ose hyrjet crisp, por daljet që prodhon janë pothuajse gjithmonë fuzzy set. Kur FIS përdoret si kontroller, është e nevojshme që të ketë një dalje crisp. Prandaj në këtë rast përshtatet metoda e defuzzification për të përftuar një vlerë crisp që paraqet më së miri një fuzzy set.

4.7.3 Funksionimi i sistemit të inference fuzzy

Ky sistem konsiston në një ndërfaqe fuzzification, një bazë rregullash, një bazë të dhënash, një njësi të marrjes së vendimeve dhe një ndërfaqe defuzzification si në figurën 4.6. [47], [51]

- Baza e rregullave përfshin njohuri të fushës së aplikimit dhe qëllimet e kontrollit si dhe karakterizon qëllimet e kontrollit nëpërmjet një sërë rregullash të formës "Në qoftë se.. – Atëherë..".
- Baza e të dhënave përcakton funksionin e anëtarësimit të fuzzy sets të përdorur në rregullat fuzzy. Siguron përcaktimet e nevojshme që përdoren për përcaktimin e rregullave gjuhësore të kontrollit dhe manipulimin e të dhënave fuzzy.
- Njësia e marrjes së vendimeve kryen veprimet e inference në rregullat.
- Ndërfaqja e fuzzification transformon hyrjet crisp në nivele të përshtatshme me vlerat gjuhësore
- Ndërfaqja e defuzzification transformon rezultatet fuzzy të inference në dalje crisp.

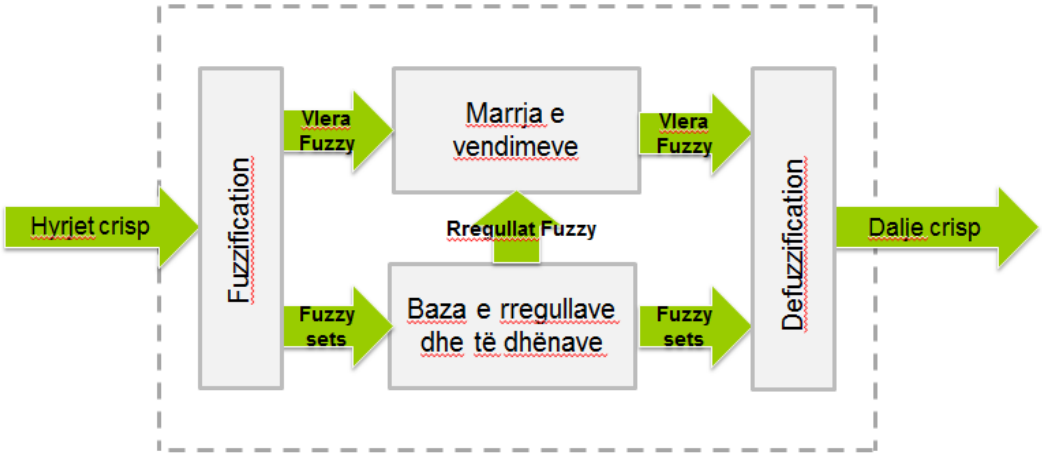


Figura 4.6. Modeli i sistemit inference

Hyrja crisp konvertohet në fuzzy duke përdorur metodën e fuzzification. Pas fuzzification formohet baza e rregullave. Baza e rregullave dhe baza e të dhënave së bashku njihen si baza e njohurive. Defuzzification përdoret për të konvertuar vlerën fuzzy në vlerë reale që është dalja. Hapat e arsyetimit fuzzy të kryer nga FIS janë:

1.Krahason variablat hyrës me funksionet e anëtarësimit në pjesën e mëparshme
për të marrë vlerat e anëtarësimit të çdo emërtimi gjuhësor (ky hap quhet fuzzification).

2.Kombinon (nëpërmjet një operatori të caktuar t-norm, zakonisht shumëzim ose minimum) vlerat e anëtarësimit të pjesës paraprake për të marrë forcën e ndezjes së çdo rregulli.

3.Gjeneron pasojat e përshtatshme (fuzzy ose crisp) ose çdo rregull në varësi të forcës së ndezjes.

4.Mbledh pasojat e përshtatshme për të përftuar daljen crisp (defuzzification).

4.8 Metodat e fuzzy inference

Dy tipet kryesore të metodave të fuzzy inference janë metoda e fuzzy inference Mamdani që është më e përdorshme. [42], [45] Kjo metodë u paraqit nga Mamdani dhe Assilian (1975). Një metodë tjetër e njohur është metoda Sugeno ose Takagi-Sugeno-Kang e procesit të fuzzy inference. Kjo metodë u paraqit nga Sugeno (1985). Quhet dhe metoda TS. Diferenca kryesore ndërmjet dy metodave qëndron në rezultatin e rregullave

fuzzy. Sistemet Mamdani përdorin fuzzy sets si rezultat i rregullit ndërsa sistemet fuzzy TS përdorin funksionet lineare të variablave të hyrjes si rezultat ose konkluzion të rregullit.

4.8.1 Metoda Mamdani

Kjo është metoda më e përdorur. Eshtë ndër sistemet e para të kontrollit të ndërtuar duke përdorur teorinë e fuzzy set. U propozua nga Mamdani (1975) si një përpjekje për të kontrolluar një kombinim të boilerit me një motor me avull duke sintetizuar një set të rregullave gjuhësore të kontrollit të marra nga operatorët njerëzor me experience. Përpjekja e Mamdanit është bazuar në botimet e Zadeh (1973) mbi algoritmat fuzzy për sistemet kompleksë dhe proceset e vendimit. Mamdani inference, siç është përcaktuar për logjikën fuzzy, pret që funksionet e anëtarësimit të daljes të jenë fuzzy sets. Pas procesit të grumbullimit, për çdo variabël dalje ka një fuzzy set që duhet të defuzzified. Në të shumtën e rasteve është më eficiente të përdoret një spike e vetme si funksion anëtarësimi të daljes në vend të një fuzzy set të shpërndarë. Kjo rrit efikasitetin e procesit të defizzification sepse thjeshton llogaritjen e kërkuar nga metoda e përgjithshme Mamdani, e cila gjen qendrën e masës të një funksioni dy-dimensional. Në vend të integrimit të funksionit dy–dimensional për të gjetur qendrën e masës përdoret mesatarja e ponderuar e disa pikave të dhëna. Sistemet Sugeno mbështesin këtë model.

Në përgjithësi sistemet Sugeno mund të përdoren për modelimin e një sistemi inference në të cilin funksionet e anëtarësimit janë linearë ose konstant. Në modelin Mamdani Fuzzy, operatori i bashkimit ose lidhjes është *min*, *t-norm* nga rregullat e kompozuara është *min* dhe për agregimin e rregullave përdoret operatori *max*.

Për të llogaritur daljen e një sistemi inference ndiqen këto hapa:

- Përcaktohet një set i rregullave fuzzy
- Fuzzification
- Vlerësimi i rregullave
- Agregimi i daljeve të rregullit
- Defuzzification

4.8.2 Metoda Tagaki- Sugeno

Modeli fuzzy Sugeno u propozua nga Takagi, Sugeno, dhe Kang në një përpjekje për të formalizuar një model të sistemit për të gjeneruar rregullat fuzzy nga një grup të dhënash hyrje-dalje. Sugeno sugjeroi përdorimin e një "spike", një "singleton", si funksion anëtarësimi të daljes së rregullit. Një fuzzy singleton, është një fuzzy set me një FA që është "njësi" në një pike të veçantë të universit dhe zero kudo tjetër. Ky model ndryshon nga modeli Mamdani në daljen e rregullit. Në vend të një fuzzy set ai përdor një funksion matematikor të variablave të hyrjes.

Ky model njihet gjithashtu si modeli Sugeno-Takagi. Një rregull tipik fuzzy në këtë model fuzzy ka formën:

" Nqs x është A dhe y është B atëhere z=f(x,y)",

Ku A, B janë fuzzy sets në hyrje; z=f(x,y) është një funksion crisp në dalje.

Zakonisht f(x,y) është një polinomial në variablat e hyrjes x dhe y, por mund të jetë një funksion tjetër që mund të përshkruajë në mënyrë të përshtatshme daljen e sistemit brenda zonës fuzzy të specifikuar nga hyrja e rregullit. Kur f(x,y) është polinomial i rendit të parë, kemi modelin fuzzy Sugeno të rendit të parë. Kur f është konstant, kemi modelin fuzzy Sugeno të rendit zero, i cili mund të shihet si rast i veçantë i Mamdani FIS ku çdo dalje e rregullit specifikohet nga një singleton fuzzy, ose rast i veçantë i modelit Tsukamoto ku çdo dalje e rregullit specifikohet nga një funksion anëtarësimi i funksionit shkallë i përqendruar në konstant.

Modeli Sugeno i rendit zero është më i përdorur dhe zakonisht ka këtë formë:

Nqs x është A dhe y është B atëhere z është k *Ku k është konstante*

Dy pjesët e para të procesit të inference fuzzy, fuzzification i hyrjeve dhe aplikimi i operatorit fuzzy janë të njëjta. Diferenca kryesore ndërmjet Mamdani dhe Sugeno është që funksionet e anëtarësimit të daljes janë linearë ose konstant.

Për shkak të varësisë lineare të çdo rregulli të variablave hyrëse të sistemit, metoda Sugeno është ideale për të vepruar si një mbikëqyrës interpolimi i kontrollerave të shumëfishtë lineare për t'u aplikuar respektivisht në kushte operimi të ndryshme të një sistemi dinamik jolinear.

4.8.3 Krahasimi ndërmjet metodës Mamdani dhe Sugeno

Modeli Mamdani përdor teknikën e defuzzification të një dalje fuzzy ndërsa modeli Sugeno përdor mesataren e ponderuar për të llogaritur daljen crisp.

Ndryshimi ndërmjet dy metodave është që funksionet e anëtarësimit të daljes së Sugeno janë linearë konstant. Gjithashtu një ndryshim qëndron në daljet e rregullave fuzzy të tyre, dhe kështu grumbullimi i tyre dhe defuzzification ndryshojnë dukshëm. Numri i fuzzy sets të hyrjes dhe rregullat fuzzy të nevojshme nga sistemi Sugeno varet nga numri dhe vendndodhjet e ekstremeve të funksionit që do përafrohet. Në metodën Sugeno kërkohet një numër i madh i rregullave fuzzy për të përafruar funksionet periodike dhe oshilimet e forta.

Konfigurimi minimal i sistemeve TS mund të reduktohet dhe të bëhen më të vogla se ato të sistemeve Mamdani nqs përdoren fuzzy sets të hyrjes jo trapezoidal dhe jo trekëndor. Kontrollerat Sugeno zakonisht kanë numër të madh të parametrave të rregullueshëm në dalje të rregullit dhe ky numër rritet eksponencialisht me rritjen e numrit të variablave të hyrjes. Egzistojnë më pak rezultate matematikore për kontrollerat TS sesa për ato Mamdani sidomos për kontrollerat e qëndrueshmërisë së sistemit. Mamdani është më i lehtë për t'u ndërtuar se metoda Sugeno apo TS.

Avantazhet e Metodës Sugeno,

- Është më efikas në llogaritje
- Funksionon mirë me teknikat lineare
- Funksionon mirë me teknikat e optimizimit dhe përshtatjes
- Garanton vazhdimësinë e sipërfaqes së daljes
- Është e përshtatshme për analizën matematike.

Avantazhet e Metodës Mamdani

- Është intuitive
- Ka pranim të gjerë.
- Ajo mer parasysh dhe hyrjet nga njerëzit.

Sistemi i inferences është më i rëndësishmi në teorinë e fuzzy set. Janë ndërtuar nga ekspertë dhe janë përdorur në automatikë, në analizën e vendimeve dhe sistemet të tjerë eksperte.

4.9 Baza e njohurive të kontrollit

Detyrat kryesore në ndërtimin e njohurive bazë të kontrollit janë: Së pari, mund të përzgjidhen një grup i variablave gjuhësorë të cilët përshkruajnë vlerat e parametrave kryesorë të kontrollit të procesit. [49], [50] Parametrat e hyrjes dhe daljes mund të përcaktohen nga ana gjuhësore në këtë fazë duke përdorur termin e duhur të grupit. Përzgjedhja e nivelit të kokrrizimit të një termi për një variabël hyrje ose dalje luan një rol të rëndësishëm në cilësinë e kontrollit. Së dyti, baza e njohurive të kontrollit mund të zhvillohet duke përdorur përshkrimin e mësipërm gjuhësor të parametrave të hyrjes dhe daljes. Sugjerohen katër metoda për këtë:

- njohuritë dhe eksperienca e ekspertit
- modelimi i veprimit të kontrollit të operatorit
- modelimi i procesit
- vet organizimi

Nga këto metoda më e përdorur është e para. Kjo metodë është efektive kur operatorët ekspertë njerëzorë mund të shprehin njohuritë që përdorin në kontrollin e procesit në rregulla të formës “Në qoftë se .. – Atëherë..”.

Metoda e dytë modelon direkt veprimet e kontrollit të operatorit. Tipet e veprimeve të kontrollit që merren nga operatori janë të modeluara.

Metoda e tretë ka të bëjë me modelimin fuzzy të një procesi ku një model i përafërt i impiantit konfirmohet duke përdorur implikime të cilat përshkruajnë gjendjet e mundshme të sistemit. Në këtë metodë zhvillohet një model dhe ndërtohet një kontroller fuzzy për kontrollin e modelit fuzzy, duke e bërë këtë model të ngjashëm me modelin e marrë në teorinë e kontrollit. Prandaj janë të nevojshëm identifikimi i parametrave dhe strukturës së proceseve.

Metoda e katërt i referohet kërkimeve të Procyk dhe Mamdani. Idea kryesore në këtë metodë është zhvillimi i rregullave të cilat mund të rregullohen me kalimin e kohës për të përmirësuar performancën e kontrollerit. Kjo metodë është e ngjashme me përdorimin e rrjetave neurale në ndërtimin e njohurive bazë të një kontrolleri logjik fuzzy.

4.10 Marrja e vendimeve fuzzy

Marrja e vendimeve dhe kontrolli janë dy fusha me metoda të përcaktuara për zgjidhjen e problemeve dhe janë shumë të lidhura me njëra tjetrën.

Marrja e vendimeve është në thelb një aspekt i rëndësishëm në të gjitha aspektet e jetës dhe është veprimtaria themelore e qenieve njerëzore. [42] Në çdo proces vendimmarrje merret në konsideratë informacioni në lidhje me rezultatet dhe zgjidhet midis dy ose më shumë alternativave për veprim të mëvonshëm. Nga vendimet e duhura që merren, atëherë pritet një dalje e mirë. Një vendim i marrë është i sigurtë, kur dalja për çdo veprim mund të përcaktohet saktësisht.

Ka disa mënyra në të cilat mund të merren vendimet fuzzy.

Radhitja fuzzy: përfshin vendimin e marrë në bazë të radhës. Cili ka radhën i pari, i dyti etj. Nqs x1=2 , x2=5, atëhere x2>x1, këtu nuk ka pasiguri dhe është radhitje crisp. Kur futet pasiguria ose paqartësia atëhere quhet radhitja fuzzy ose radhitja sipas radhës. Në qoftë se pasiguria në radhë është e rastësishme, atëhere përdoret funksioni i densitetit probabilitar

Vendim marrja individuale: Situata e vendimit në këtë model karakterizohet nga:

- set i veprimeve të mundshme
- set i qëllimeve $p_i (i \in x_n)$, i shprehur në terma të fuzzy set
- set i kufizimeve $Q_j (j \in x_m)$, i shprehur në terma të fuzzy set

Zakonisht fuzzy sets shprehin qëllimet dhe kufizimet në këto formulime.

Vendim marrja nga shumë persona: Ndryshon nga ajo individuale në:

1. Qëllimet e marrësve të vendimit individual ndryshon, në atë që secili vendos një rregull të ndryshëm renditje

2. Marrësit individual të vendimit kanë akses në informacione të ndryshëm mbi të cilët mund të bazojnë vendimin e tyre

Vendim marrja me shumë objektiva: Procesi përfshin përzgjedhjen e një alternative a_i, nga disa alternativa A, duke patur parasysh një set, le të themi {0} objektiva që është i rëndësishëm për një vendim marrës.

Për një univers me n alternativa: $A = \{a_1, a_2, ... a_n\}$ dhe setin me "r" objektiva $O = \{O_1, O_2, ... O_r\}$. Funksioni i vendimit (DF) jepet si ndërprerje e gjithë objektivave $DF = O_1 \wedge O_2 \wedge .... \wedge O_r$ dhe anëtarësia për alternativën jepet: $\mu DF(a^*) = \max_{a \in A}(\mu DF(a))$.

KAPITULLI 5

SISTEMET E PROPOZUAR

5.1 Aplikimi i fuzzy logic (FL) për kontroll

Aftësia e fuzzy sets dhe mundësia teorike e modelimit gradual të karakteristikave të rrjetit, si dhe informacioni i mbushur me pasiguri dhe paqartësi e bën fuzzy logic mjaft të përdorshëm në shumë aplikime.

Në sistemet FC, njohuritë e ekspertëve kodohen në formën e rregullave fuzzy, të cilat përshkruajnë veprimet e rekomanduara për klasa të ndryshme të situatave të paraqitura nga fuzzy sets. Në fakt, mund të modelohet çdo lloj ligji kontrolli nga metodologjia fuzzy, me kusht që ky ligj të shprehet me terma të rregullave "Në qoftë se …. – Atëherë..", si në rastin e sistemeve ekspertë. Megjithatë Fuzzy logic (FL) ndryshon nga modelet e sistemeve ekspertë pasi ofron një mekanizëm interpolimi nga disa rregulla. Ky model mund të jetë më praktik për të marrë njohuritë nga ekspertët sesa të llogarisë një kontroll optimal për shkak të kostos së modelimit apo ngaqë nuk mund të arrihet modeli.

Një koncept që luan një rol të rëndësishëm në aplikimin e FL është variabli gjuhësor. Variablat gjuhësorë mund të shihen si kompresim i të dhënave. Një variabël gjuhësor mund të paraqesë disa variabla numerikë.

Kontrolleri fuzzy përshkruan algoritmin për kontrollin e procesit si një lidhje fuzzy ndërmjet informacionit mbi kushtet e procesit që do kontrollohet dhe daljes së procesit.

Në sistemet e propozuar kontrolleri fuzzy përdoret për të përcaktuar besueshmërinë e nyjeve dhe duke u bazuar në parametrat e hyrjes si numri i nyjeve në cluster, humbja e paketave, fuqia e shpenzuar dhe siguria, përcakton në dalje nëse nyja është e besueshme apo jo.

Detyrat kryesore në ndërtimin e njohurive bazë të kontrollit janë:

Së pari, përzgjidhen një grup i variablave gjuhësorë të cilët përshkruajnë vlerat e parametrave kryesorë të kontrollit të procesit. Parametrat e hyrjes dhe daljes mund të përcaktohen nga ana gjuhësore në këtë fazë duke përdorur termin e duhur të grupit.

Për parametrat e zgjedhur në sistemet e propozuar janë zgjedhur variablat gjuhësorë që mendojmë që paraqesin më së miri këto parametra. Variablat gjuhësorë të zgjedhur jepen në paragrafët në vijim.

Përzgjedhja e nivelit të kokrrizimit të një termi për një variabël hyrje ose dalje luan një rol të rëndësishëm në cilësinë e kontrollit (janë zgjedhur në sistemet e propozuar duke u bazuar në logjikë). Së dyti, baza e njohurive të kontrollit mund të zhvillohet duke përdorur përshkrimin e mësipërm gjuhësor të parametrave të hyrjes dhe daljes.

Fuzzification është një koncept i rëndësishëm i teorisë së logjikës fuzzy. Fuzzification është procesi i konvertimit të vlerave crisp në fuzzy. Vlerat fuzzy formohen duke identifikuar disa pasiguri prezente në vlerat crisp. Konvertimi i vlerave fuzzy paraqitet nga funksionet e anëtarësimit. Funksioni i anëtarësimit është paraqitja grafike e fuzzy set-ve. Në sistemin tonë përdorim funksionet e anëtarësimit trekëndor dhe trapezoidal duke qenë se paraqesin më mirë variablat e hyrjes të sistemit dhe janë më të thjeshtë.

Funksioni trekëndor përcaktohet nga:

$$\mu_A(x) = \max(\min(\frac{x-a}{m-a}, 1, \frac{b-x}{b-m})) \quad (4.10)$$

Funksioni trapezoidal përcaktohet nga:

$$\mu_A(x) = \max(\min(\frac{x-a}{b-a}, 1, \frac{d-x}{d-c})) \quad (4.11)$$

Sistemi i inference është pjesa logjike e FLC. Ky sistem bazohet në rregullat e formës “Në qoftë se … - Atëherë…”. Për përcaktimin e daljeve të çdo rregulli si dhe për agregimin e daljeve të rregullave përdoren veprimet logjike “OSE” (OR) ose “max”dhe “EDHE” (AND) ose “min” ndryshe quhet kompozimi max-min. Dalja e sistemit të inference është fuzzy. Ne përdorim modelin Mamdani për procesin e inference në

sistemin tonë. Në modelin Mamdani Fuzzy, për rregullat përdoret operatori i bashkimit AND ose *min*, dhe për agregimin e rregullave përdoret operatori OSE ose *max*.

Për ta bërë këtë dalje fuzzy të përshtatshme për aplikimet reale nevojitet procesi i defuzzification. Defuzzification ka si qëllim konvertimin e daljes fuzzy në dalje të crisp të objektivit të kontrollit. Kujtojmë që dalja fuzzy është variabël gjuhësor i cili duhet të konvertohet në vlerë crisp nëpërmjet procesit të defuzzification. Për sistemin tonë për procesin e defuzzification përdorim metodën e qendrës së zones (COA), pasi metoda e defuzzification duhet të jetë e njëjtë me atë të përdorur në fuzzification. Në rastin tonë për funksionet e zgjedhur të anëtarësimit kjo është metoda e përshtashme.

Metoda COA llogarit qendrën e gravitetit të shpërndarjes për veprimin e kontrollit sipas formulës.

$$Z^* = \frac{\sum_{j=1}^{q} z_j \mu_C(z_j)}{\sum_{j=1}^{q} \mu_C(z_j)} \qquad (4.14)$$

Marrja e vendimeve është një pjesë e rëndësishme e gjithë sistemit. Sistemi i inference fuzzy formulon rregulla të përshtatshme dhe në bazë të rregullave merret vendimi.

5.2 Sistemi i propozuar 1 (F2SMC1)

Në këtë punim nuk propozohet një protokoll i ri i sigurtë për MANET, por propozohet një sistem i bazuar në fuzzy logic për të përcaktuar dhe vlerësuar besueshmërinë e nyjeve cluster në MANET. Simulimet janë bërë duke përdorur Fuzzy Logic Toolbox në Matlab. [53]

Rrjeti MANET i bazuar në clustering mund të jetë çdo lloj rrjeti i përbërë nga nyje heterogjene me karakteristika të caktuara, mbi bazën e të cilave do bëhet vlerësimi i besueshmërisë së këtyre nyjeve. Sistemi i propozuar vlerëson çdo nyje të cluster-it të rrjetit, pra implementohet në çdo cluster dhe vlerëson çdo nyje brenda tij. Karakteristikat e nyjeve që merren në hyrje janë vlerësuar nga algoritme apo protokolle të tjerë, ne i fusim në sistemin tonë si parametra hyrje mbi të cilët bëjmë vlerësimin e besueshmërisë me anë të sistemit FLC.

Modeli i sistemit F2SMC1 jepet në figurën 5.1. Konsiderojmë tre paramtera në hyrje: Numri i nyjeve në cluster (NNC), Humbja e paketave (PL), Fuqia e shpenzuar (SP). Në dalje vlerësohet besueshmëria e nyjeve dhe si parameter dalje konsiderohet nyja mbetet në cluster ose nyja largohet nga cluster-i (R/L). Këto parametra nuk janë të lidhur me njëri tjetrin, prandaj mund të përdorim sistemin fuzzy.

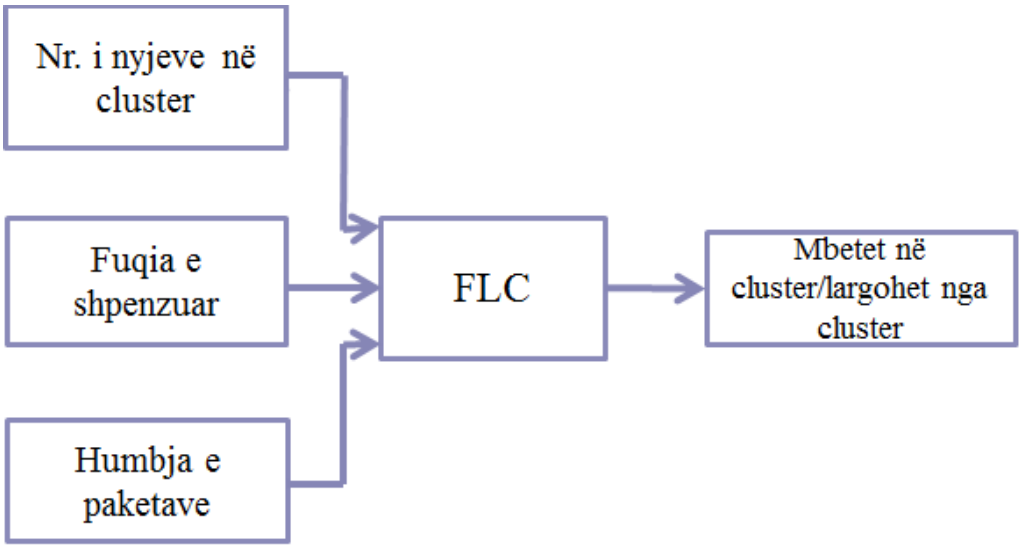


Figura 5.1. Modeli i sistemit F2SMC1

5.3 Procedura për vlerësimin e besueshmërisë së nyjeve cluster

Për vlerësimin e besueshmërisë së nyjeve cluster në MANET ndiqen këto hapa. Duhet të përcaktohen fillimisht parametrat e hyrjes, në sistemin tonë kemi tre parametra të cilët ndikojnë në performancën e rrjetit: Numri i nyjeve në cluster (NNC), Humbja e paketave (PL), Fuqia e shpenzuar (SP). Theksojmë që përcaktimi i parametrave të hyrjes dhe dalja varet nga eksperienca njerëzore mbi rrjetin ose sistemin. Këto parametra ndikojnë në performancën e rrjetin dhe nuk janë të lidhur me njëri tjetrin, prandaj mund të përdorim sistemin fuzzy logic. Pasi përcaktohen parametrat e hyrjes përcaktohet dhe parametri që do vlerësohet në dalje. Në sistemin tonë në dalje vlerësohet besueshmëria e nyjeve në cluster në MANET e shënuar Mbetet në cluster/Largohet nga cluster (R/L). Kjo do të thotë që nëse nyja është e besueshme mbetet në cluster dhe merr pjesë në transmetimin e paketave, dhe nëse nyja nuk është e besueshme largohet nga cluster dhe

nuk merr pjesë në transmetimin e paketave. Për parametrat e hyrjes dhe daljes përcaktohen në hapin e dytë variablat gjuhësorë që përfaqësojnë këto parametra. Për parametrat e zgjedhur në sistemin tonë kemi përcaktuar variablat gjuhësorë përkatësisht si më poshtë (theksojmë që dhe variablat gjuhësorë përzgjidhen nga intuita njerëzore):

Numri i nyjeve në cluster (NNC) = {i vogël, Mesatar, i madh}={Fe, Mi, Ma};

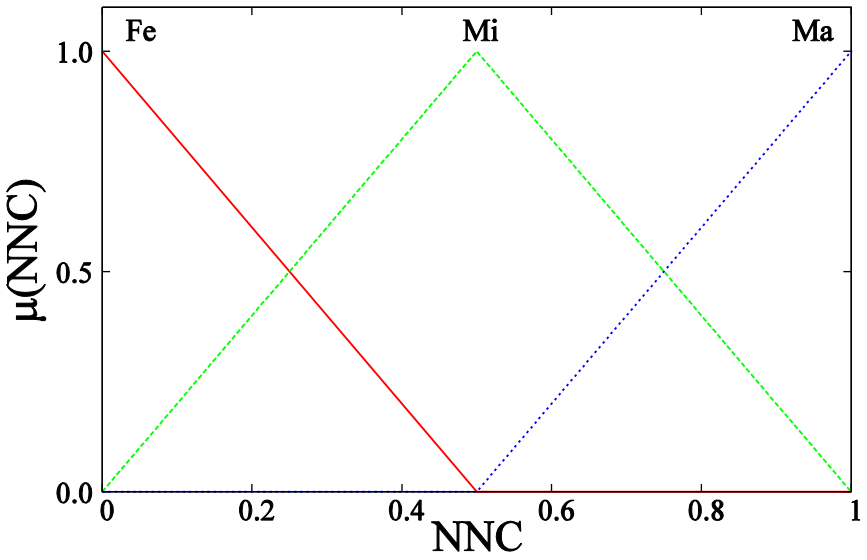
Fuqia e shpenzuar (SP) = {Pak, Mesatare, Shumë}= {L, M, H};

Humbja e paketave (PL) = {E ulët, Mesatare, E lartë}={Few, Mid, Hi};

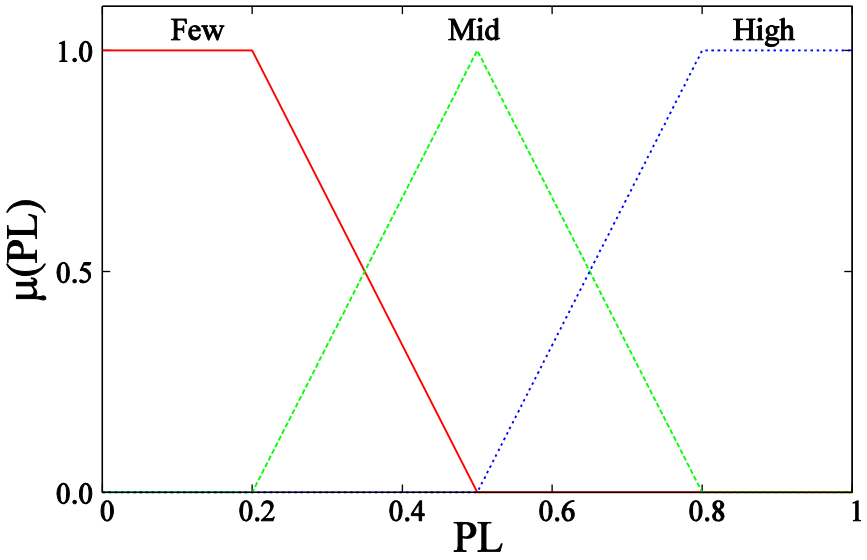
Dhe për daljen përdoren termat si më poshtë:

Mbetet në cluster/Largohet nga cluster (R/L) = {Mbetet, Mbetet pak, Nuk mbetet Nuk largohet, Largohet pak, Largohet}= {Re, WRe, NReNL, WLe, Le }

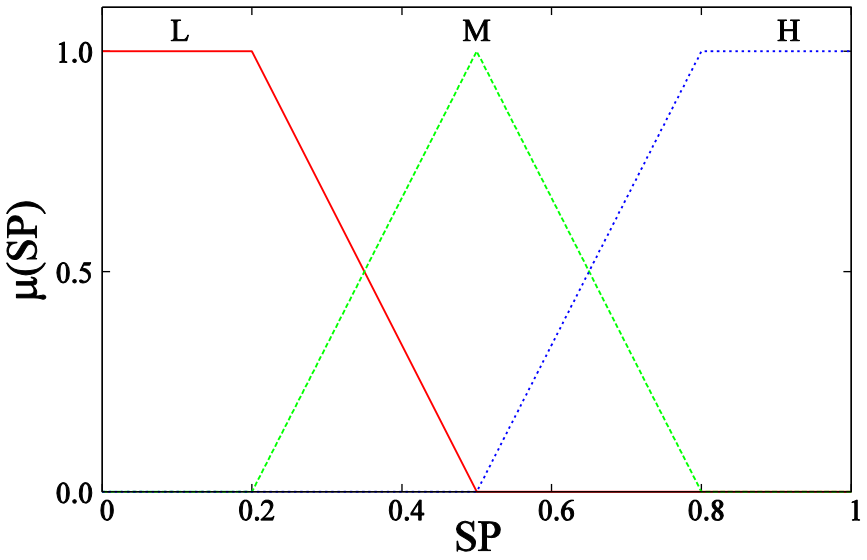
Pas përcaktimit të variablave gjuhësorë për parametrat e hyrjes dhe daljen, përcaktohen funksionet e anëtarësimit për secilin prej tyre. Përdorim funksionet e anëtarësimit trekëndor dhe trapezoidal përzgjedhja e të cilëve bëhet në mënyrë logjike gjatë simulimeve, shihet se ku përputhen më mirë dy nga tre parametrat e zgjedhur. Zgjedhja e pikës së prerjes së dy trekëndëshave (funksionet e anëtarësimit për secilin variabël gjuhësor) bëhet në mënyrë logjike gjatë simulimeve duke vendosur pikën më të mirë të prerjes që të përfaqësohen të gjitha variablat e zgjedhur. Në figurën 5.2 tregohen funksionet e anëtarësimit për parametrat e hyrjes dhe daljen.



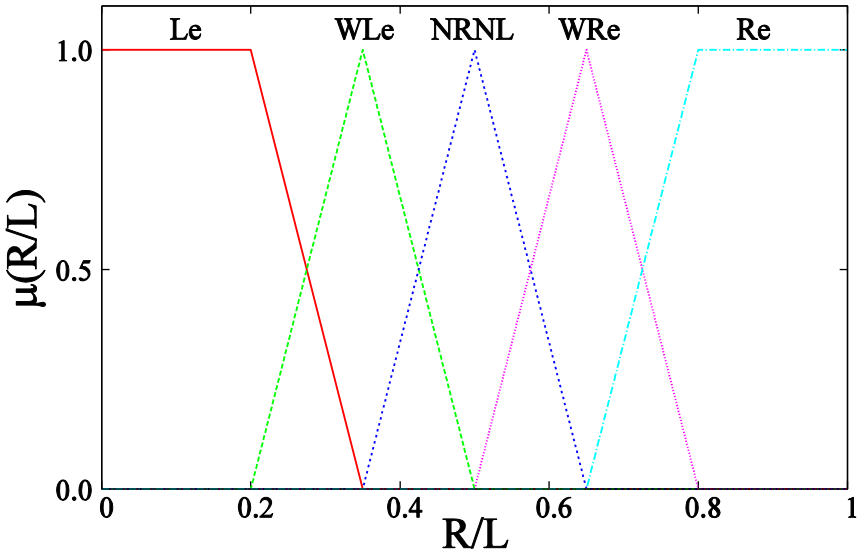
a. Numri i nyjeve në një cluster



b. Humbja e paketave



c. Fuqia e shpenzuar



d. Dalja, Mbetet/Largohet

Figura 5.2. Funksionet e anëtarësimit për parametrat e hyrjes dhe daljen

Hapi tjetër është ndërtimi i tabelës së rregullave. Për sistemin F2SMC1 kemi tre parametra në hyrje, dhe tabela e rregullave përbëhet nga 27 rregulla të cilat jepen më poshtë në tabelën 5.1.

Tabela 5.1 Tabela e rregullave fuzzy për F2SMC1

Nr. i rregullit	NNC	PL	SP	R/L
1	Fe	L	Few	Re
2	Fe	L	Middle	Re
3	Fe	L	High	WRe
4	Fe	M	Few	Re
5	Fe	M	Middle	NRNL
6	Fe	M	High	WLe
7	Fe	H	Few	NRNL
8	Fe	H	Middle	WLe
9	Fe	H	High	Le
10	Mi	L	Few	Re
11	Mi	L	Middle	WRe
12	Mi	L	High	NRNL
13	Mi	M	Few	WRe
14	Mi	M	Middle	WLe
15	Mi	M	High	WLe
16	Mi	H	Few	WLe
17	Mi	H	Middle	Le
18	Mi	H	High	Le
19	Ma	L	Few	Re
20	Ma	L	Middle	NRNL
21	Ma	L	High	WLe
22	Ma	M	Few	NRNL
23	Ma	M	Middle	WLe
24	Ma	M	High	Le
25	Ma	H	Few	WLe
26	Ma	H	Middle	Le
27	Ma	H	High	Le

Pasi vlerësohen rregullat, pra përcaktohen daljet e çdo rregulli, bëhet agregimi i daljeve të çdo rregulli që është dhe hapi pasardhës. Pas agregimit të daljeve kryhet procesi i defuzzification për përcaktimin e një vlere të vetme crisp në dalje e cila do

përcaktojë nëse nyja do mbetet në cluster apo do largohet nga cluster. Për sistemin tonë më e përshtatshme për defuzzification është metoda e qendrës së zonës (COA) e cila llogarit qendrën e gravitetit të shpërndarjes për veprimin e kontrollit me anë të kësaj formule. $Z^* = \frac{\sum_{j=1}^{q} z_j \mu_C(z_j)}{\sum_{j=1}^{q} \mu_C(z_j)}$ (4.14)

Llogjika e funksionimit të sistemit F2SMC1 është e tillë:

Në qoftë se numri i nyjeve në cluster është *i vogël* **dhe** humbja e paketave është *e ulët* **dhe** *fuqia e shpenzuar* është pak **atëherë** kjo nyje do të mbetet në cluster.

Në qoftë se numri i nyjeve në cluster është *i madh* **dhe** humbja e paketave është *e lartë* **dhe** *fuqia e shpenzuar* është *shumë* **atëherë** kjo nyje do të largohet nga cluster.

Për vlerësimin e rregullave përdorim operatorin "DHE" ose "Minimum", që do të thotë në dalje në rregullit merret vlera minimale e tre hyrjeve.

Ndërsa për agregimin ose grumbullimin e daljeve të çdo rregulli përdorim operatorin "OSE" ose "Maksimum", që do të thotë të meret vlera maksimale e daljeve.

Në figurën 5.2 jepen hapat që ndiqen për përcaktimin e besueshmërisë së nyjeve cluster.

Theksojmë që sistemi i propozuar implementohet në çdo cluster.

Gjithashtu kjo procedurë ndiqet për përcaktimin e secilës prej vlerave të daljes, pra për çdo vlerë dalje psh R/L = 0.4 përcaktohet nga defuzzification i agregimit të daljeve të rregullave (27 rregulla) që përcakton një vlerë crisp që është 0.4 njësi.

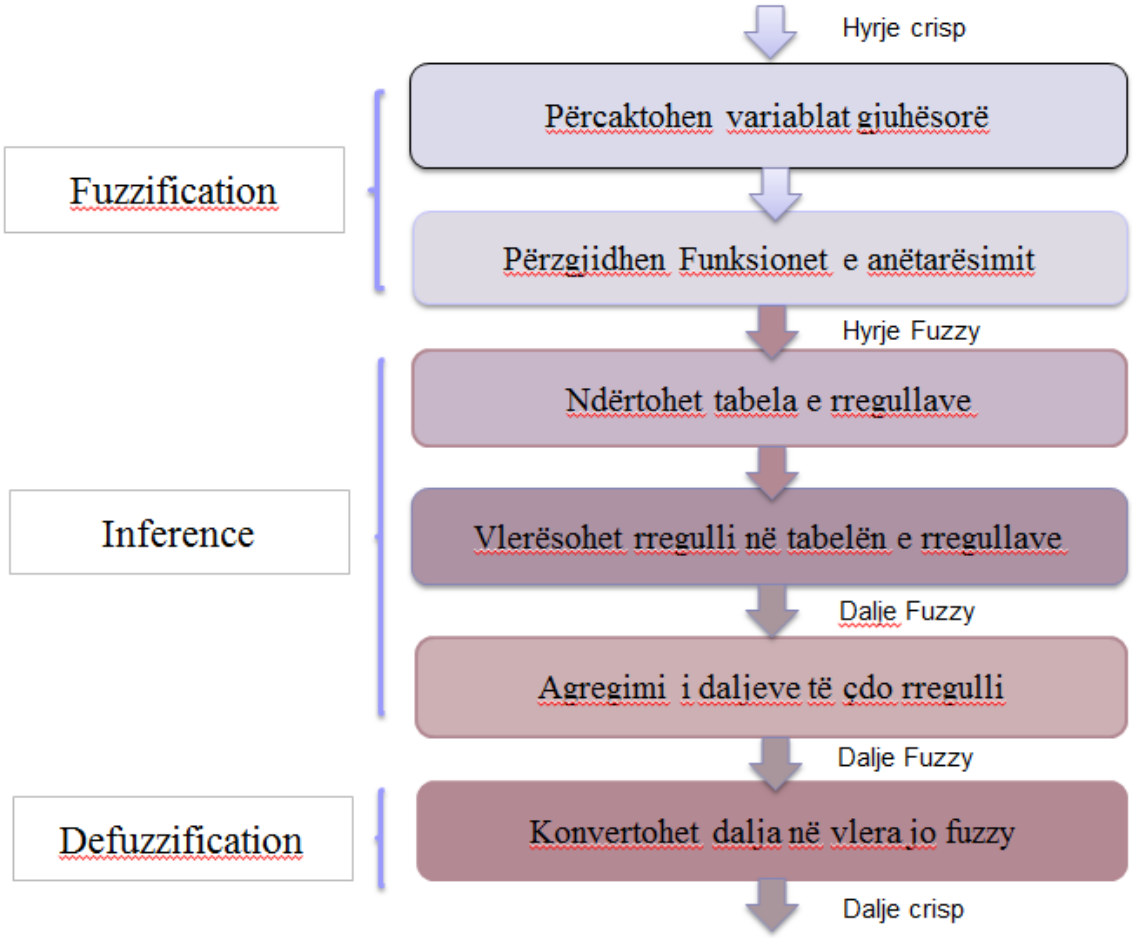
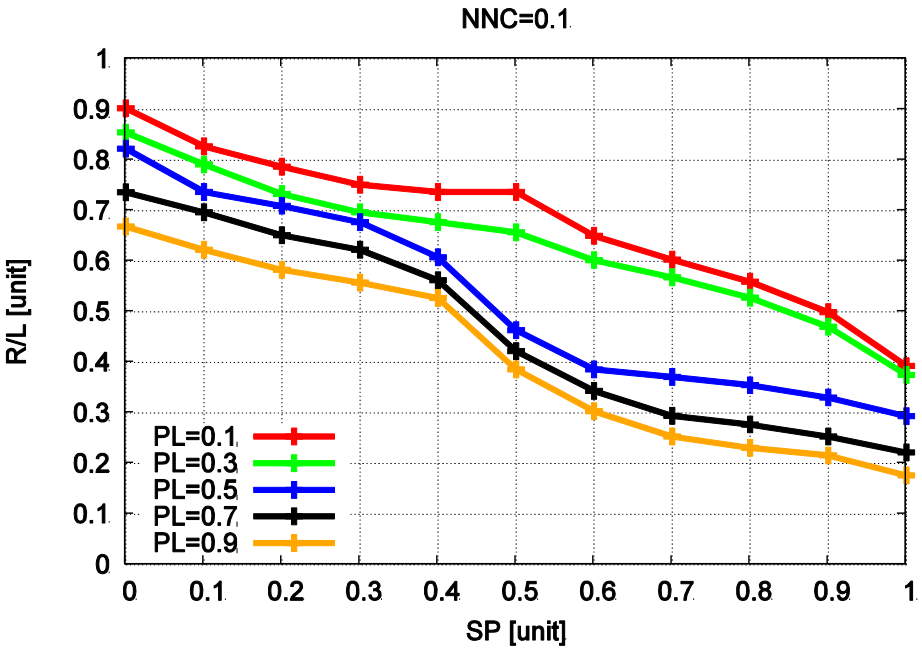


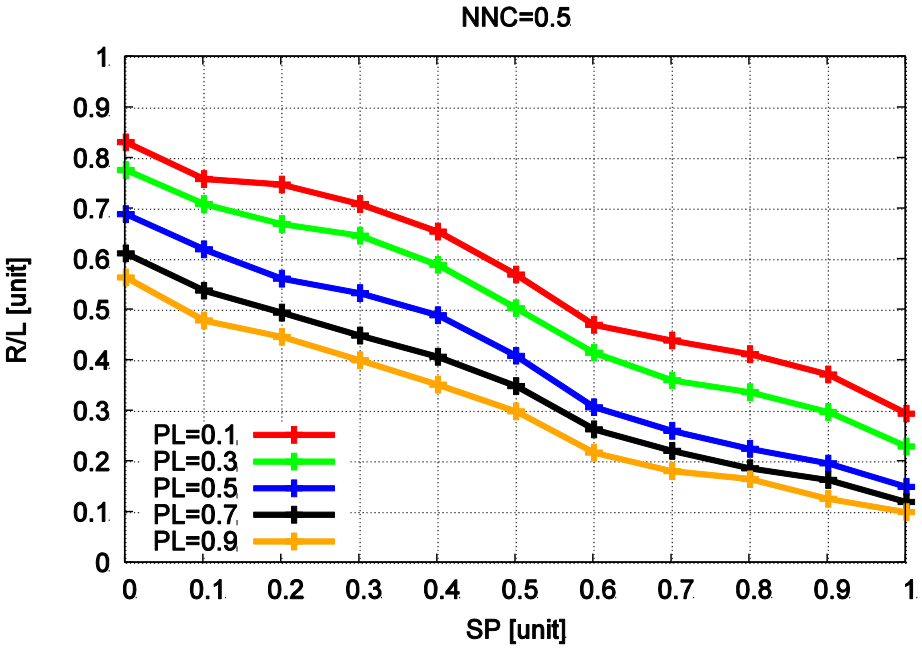
Figura 5.3. Bllokskema e procedurës për përcaktimin e besueshmërisë së nyjeve cluster

5.4 Rezultatet eksperimentale për F2SMC 1

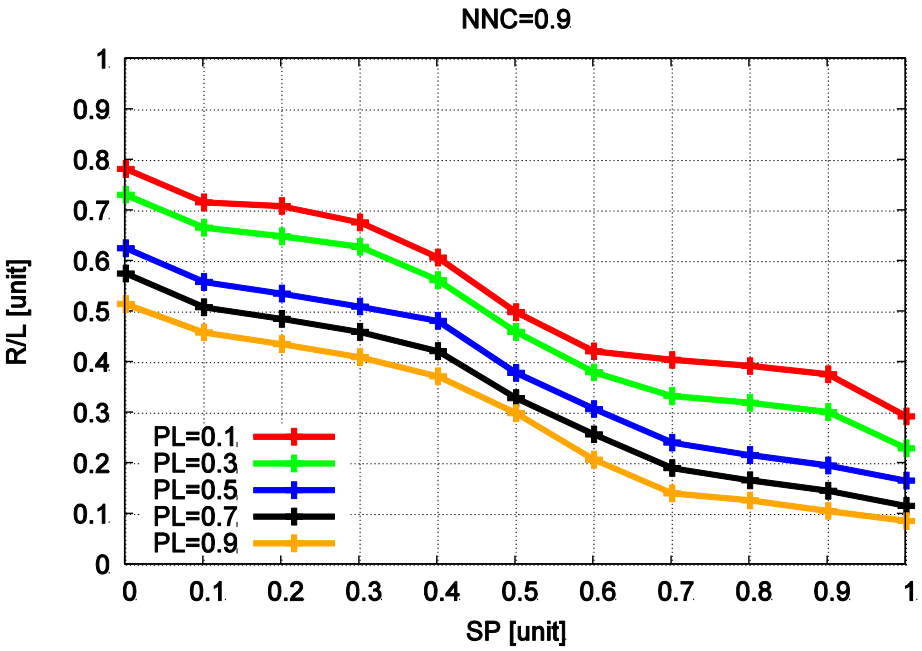
Simulimet kryhen për një cluster në MANET duke përdorur Fuzzy Logic Toolbox në Matlab. Konsiderojmë numrin e nyjeve në cluster konstant dhe studiojmë daljen e sistemit për vlera të ndryshme të dy parametrave të tjerë në hyrje, humbja e paketave (PL) dhe fuqia e shpenzuar (SP). Rezultatet e simulimeve jepen në figurën 5.4.



a. Dalja për NNC= 0.1



b. Dalja për NNC = 0.5



c. Dalja për NNC = 0.9

Figura 5.4. Dalja e sistemit F2SMC1 për NNC të ndryshëm

Në figurën 5.4.a marim vlerën NNC=0.1. Me rritjen e fuqisë së shpenzuar vihet re që dalja e sistemit zvogëlohet. Kur rritet humbja e paketave dalja gjithashtu zvogëlohet. Në figurën 5.4.b dhe 5.3.c marim NNC =0.5 dhe NNC=0.9 respektivisht. Vihet re që me rritjen e NNC dalja zvogëlohet.

Në këtë sistem konsiderojmë si parametër të besueshmërisë humbjen e paketave. Sa më e ulët të jetë humbja e paketave, aq më të besueshme janë nyjet dhe performanca e sistemit përmirësohet, pra duke zgjedhur nyjet me PL të ulët besueshmëria e sistemit rritet.

5.5 Sistemi i propozuar II (F2SMC2)

Sistemi i propozuar II (F2SMC2) është një përmirësim i sistemit F2SMC1, pasi në hyrje shtohet dhe parametri i sigurisë për nyjen. [54] Në sistemin F2SMC2 konsiderohen katër parametra në hyrje: Numri i nyjeve në cluster (NNC), Humbja e paketave (PL), Fuqia e shpenzuar (SP), Siguria (SC). Në dalje vlerësohet besueshmëria e nyjeve dhe si parametër dalje konsiderohet nyja mbetet në cluster ose nyja largohet nga cluster-i (R/L). Këto parametra nuk janë të lidhur me njëri tjetrin, prandaj mund të përdorim sistemin fuzzy. Procedura e përcaktimit dhe vlerësimit të besueshmërisë së nyjeve është e njëjti siç u shpjegua më sipër për sistemin F2SMC1.

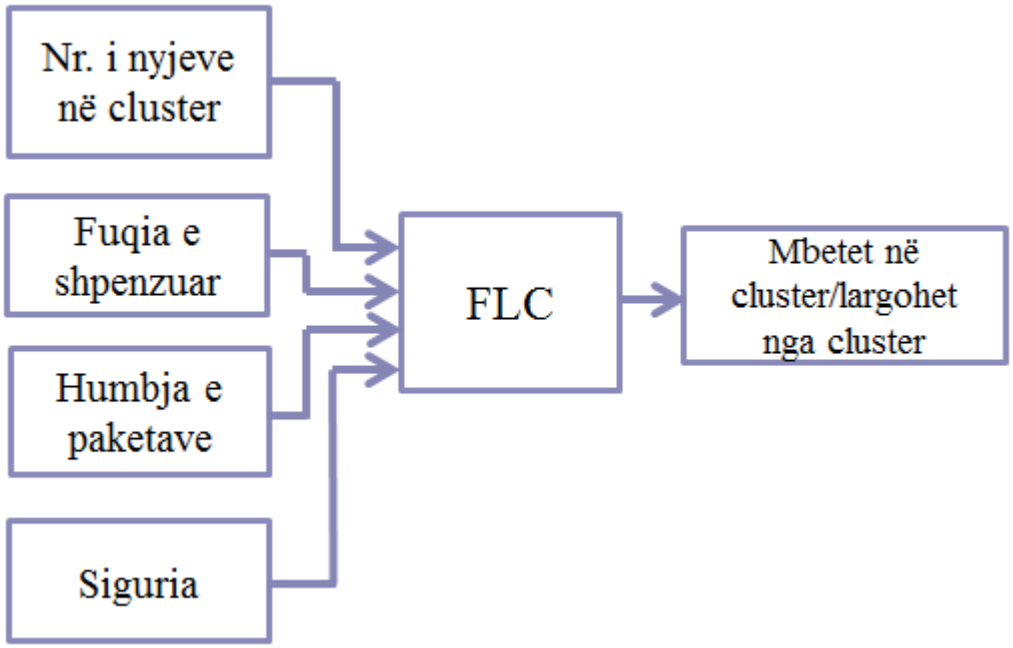


Figura 5.5. Modeli i sistemit F2SMC2

Termat e përdorur për parametrat e hyrjes janë si më poshtë:

Numri i nyjeve në cluster (NNC) = {Pak, Mesatare, Shumë}={Fe, Mi, Ma};

Fuqia e shpenzuar (SP) = {Pak, Mesatare, Shumë}= {L, M, H};

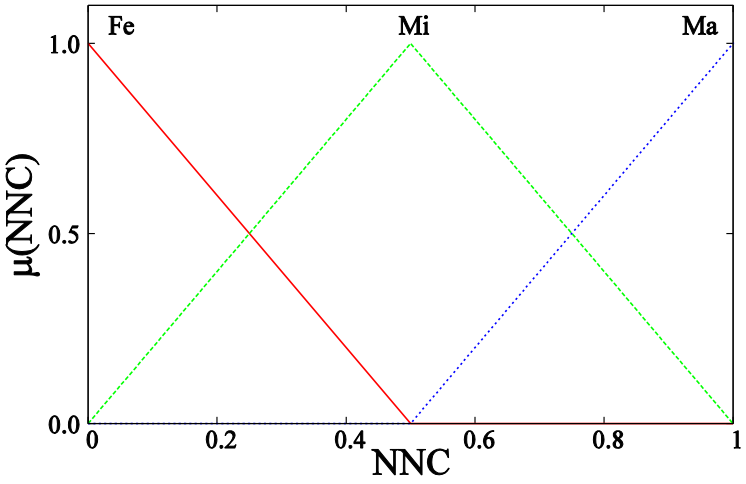
Humbja e paketave (PL) = {E ulët, Mesatare, E lartë}={Few, Mid, Hi};

Siguria (SC) = {e ulët, mesatare, e lartë} {Low, Middle, High};

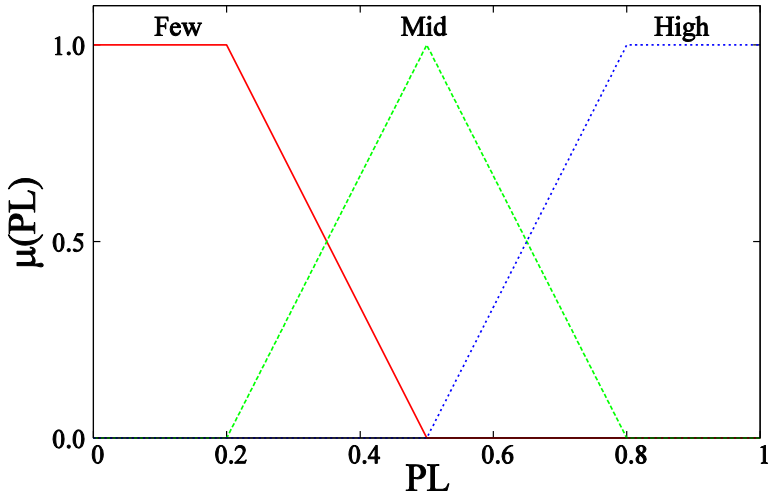
Dhe për daljen përdoren termat si më poshtë:

Mbetet në cluster/Largohet nga cluster (R/L) = {Mbetet, Mbetet pak, Nuk mbetet Nuk largohet, Largohet pak, Largohet}= {Re, WRe, NReNL, WLe, Le }

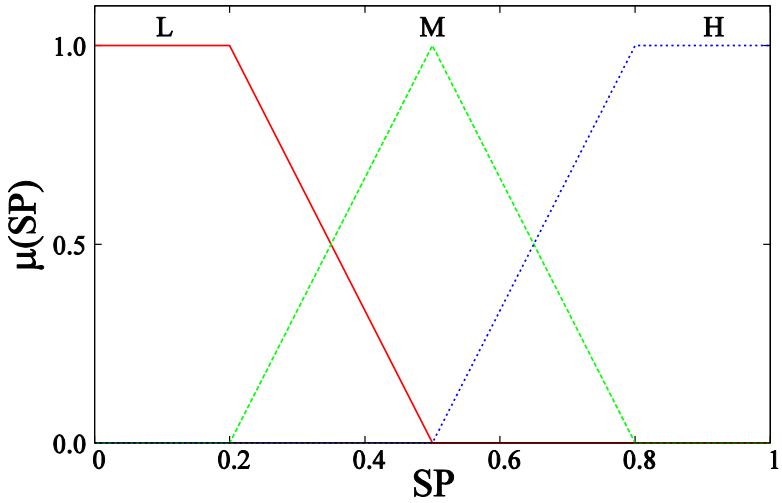
Në figurën 5.6 tregohen funksionet e anëtarësimit për parametrat e hyrjes dhe daljen.



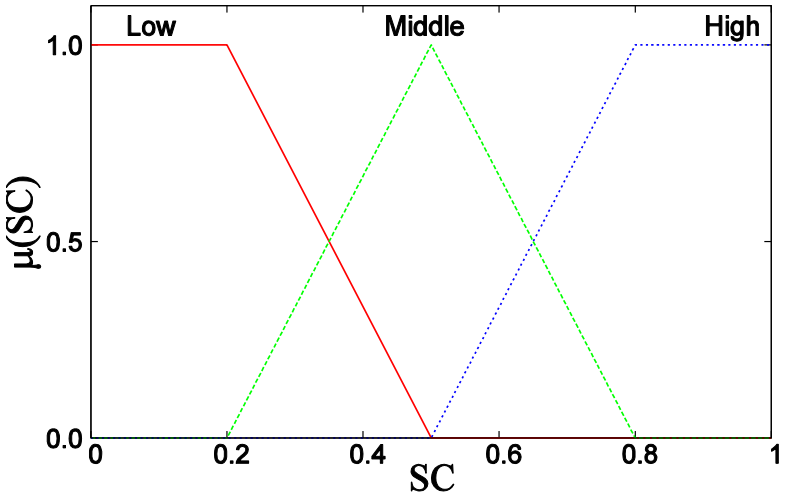
a. Numri i nyjeve në një cluster



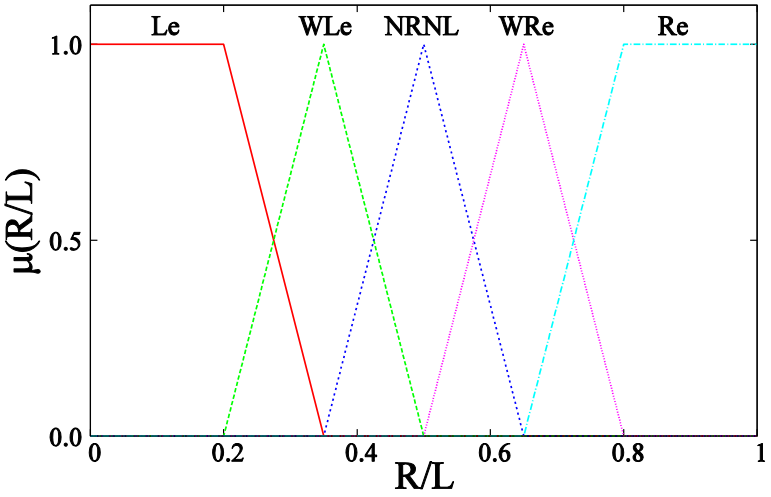
b. Humbja e paketave



c. Fuqia e shpenzuar



d. Siguria



e. Dalja e sistemit

Figura 5.6 . Funksionet e anëtarësimit për parametrat e hyrjes dhe daljen

Më poshtë jepet tabela e rregullave për sistemin F2SMC2 e cila konsiston në 81 rregulla. Sa më shumë rregulla të ketë tabela aq më saktë vlerësohet besueshmëria e nyjeve. Me rritjen e numrit të rregullave rritet saktësia e përcaktimit të besueshmërisë së

sistemit edhe pse rritet koha e simulimit. Kjo rritje e kohës justifikohet me përmirësimin që i bëhet sistemit.

Tabela 5.2. Tabela e rregullave për sistemin F2SMC2

Nr.	NNC	SP	PL	SC	R/L	Nr.	NNC	SP	PL	SC	R/L
1	Fe	L	Few	Low	WRe	41	Mi	M	Mid	Middle	WLe
2	Fe	L	Few	Middle	Re	42	Mi	M	Mid	High	WLe
3	Fe	L	Few	High	Re	43	Mi	M	Hi	Low	Le
4	Fe	L	Mid	Low	WRe	44	Mi	M	Hi	Middle	WLe
5	Fe	L	Mid	Middle	Re	45	Mi	M	Hi	High	NRNL
6	Fe	L	Mid	High	Re	46	Mi	H	Few	Low	Le
7	Fe	L	Hi	Low	NRNL	47	Mi	H	Few	Middle	WLe
8	Fe	L	Hi	Middle	WRe	48	Mi	H	Few	High	NRNL
9	Fe	L	Hi	High	WRe	49	Mi	H	Mid	Low	Le
10	Fe	M	Few	Low	WRe	50	Mi	H	Mid	Middle	Le
11	Fe	M	Few	Middle	Re	51	Mi	H	Mid	High	WLe
12	Fe	M	Few	High	Re	52	Mi	H	Hi	Low	Le
13	Fe	M	Mid	Low	WLe	53	Mi	H	Hi	Middle	Le
14	Fe	M	Mid	Middle	NRNL	54	Mi	H	Hi	High	WLe
15	Fe	M	Mid	High	NRNL	55	Ma	L	Few	Low	WLe
16	Fe	M	Hi	Low	Le	56	Ma	L	Few	Middle	Wre
17	Fe	M	Hi	Middle	WLe	57	Ma	L	Few	High	Re
18	Fe	M	Hi	High	WLe	58	Ma	L	Mid	Low	WLe
19	Fe	H	Few	Low	WLe	59	Ma	L	Mid	Middle	NRNL
20	Fe	H	Few	Middle	NRNL	60	Ma	L	Mid	High	WRe
21	Fe	H	Few	High	NRNL	61	Ma	L	Hi	Low	Le
22	Fe	H	Mid	Low	Le	62	Ma	L	Hi	Middle	WLe
23	Fe	H	Mid	Middle	WLe	63	Ma	L	Hi	High	NRNL
24	Fe	H	Mid	High	WLe	64	Ma	M	Few	Low	WLe
25	Fe	H	Hi	Low	Le	65	Ma	M	Few	Middle	NRNL
26	Fe	H	Hi	Middle	Le	66	Ma	M	Few	High	Wre
27	Fe	H	Hi	High	WLe	67	Ma	M	Mid	Low	Le
28	Mi	L	Few	Low	WRe	68	Ma	M	Mid	Middle	WLe
29	Mi	L	Few	Middle	WRe	69	Ma	M	Mid	High	NRNL
30	Mi	L	Few	High	Re	70	Ma	M	Hi	Low	Le
31	Mi	L	Mid	Low	WRe	71	Ma	M	Hi	Middle	WLe
32	Mi	L	Mid	Middle	NRNL	72	Ma	M	Hi	High	NRNL
33	Mi	L	Mid	High	WRe	73	Ma	H	Few	Low	Le
34	Mi	L	Hi	Low	WLe	74	Ma	H	Few	Middle	WLe
35	Mi	L	Hi	Middle	NRNL	75	Ma	H	Few	High	WLe

36	Mi	L	Hi	High	NRNL	76	Ma	H	Mid	Low	Le
37	Mi	M	Few	Low	NRNL	77	Ma	H	Mid	Middle	Le
38	Mi	M	Few	Middle	WRe	78	Ma	H	Mid	High	WLe
39	Mi	M	Few	High	WRe	79	Ma	H	Hi	Low	Le
40	Mi	M	Mid	Low	Le	80	Ma	H	Hi	Middle	Le
						81	Ma	H	Hi	High	WLe

5.6 Rezultatet eksperimentale për sistemin F2SMC 2

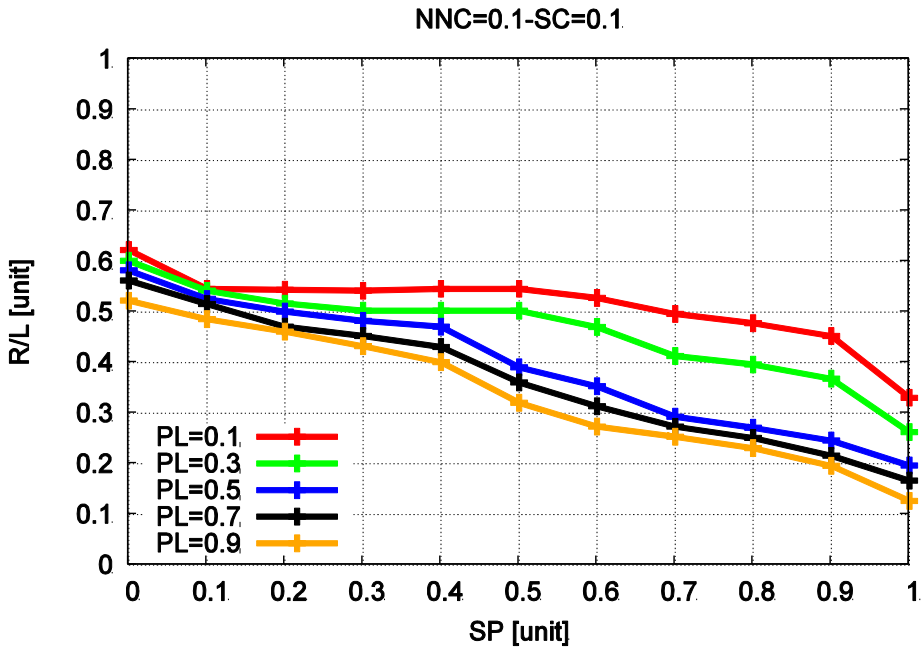
Në këtë seksion paraqiten rezultatet e simulimeve për sistemin F2SMC2. Në figurën 5.6 jepet lidhja ndërmjet parametrave NNC, SP, PL, SC dhe R/L.

Në simulime konsiderojmë NNC dhe SC si parametra konstantë. Në figurën 5.7. a, b, c, konsiderojmë NNC=0.1 dhe SC 0.1, 0.5, 0.9 respektivisht. Për shembull nqs kemi 100 nyje, 0.1 njësi do të thotë 10 nyje. Fuzzy logic punon me njësi prandaj i kemi marrë vlerat e parametrave me njësi.

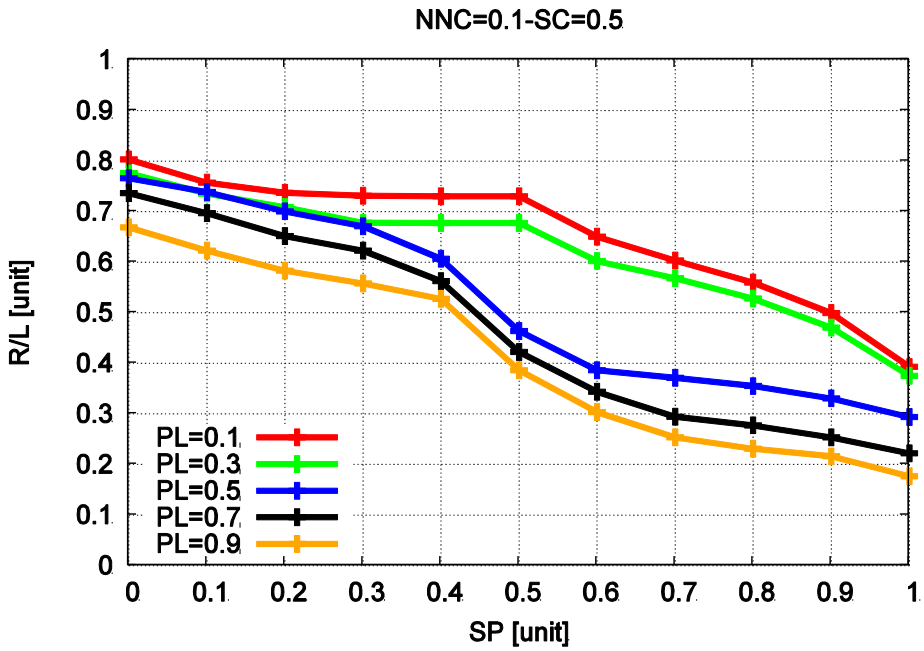
Në figurën 5.7. d, e, f konsiderojmë NNC = 0.5 njësi dhe SC 0.1, 0.5, 0.9 njësi respektivisht.

Në figurën 5.7.g, h, i konsiderojmë NNC = 0.9 njësi dhe SC 0.1, 0.5, 0.9 njësi respektivisht.

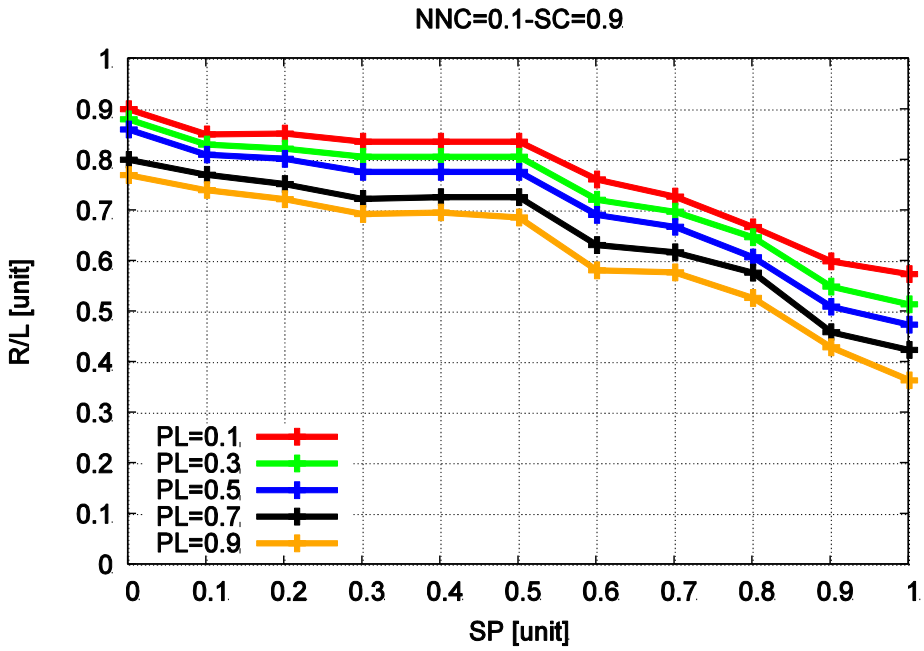
Nga rezultatet vihet re që me rritjen e numrit të nyjeve në cluster, dalja e sistemit vjen duke u zvogëluar. Dhe me rritjen e sigurisë së nyjes dalja e sistemit rritet, nyjet janë më të sigurta dhe performanca e sistemit përmirësohet. Pra duke zgjedhur nyjet me vlerë të lartë të sigurisë cluster-i (rrjeti) bëhet më i sigurtë dhe i besueshëm si dhe performanca e tij përmirësohet.



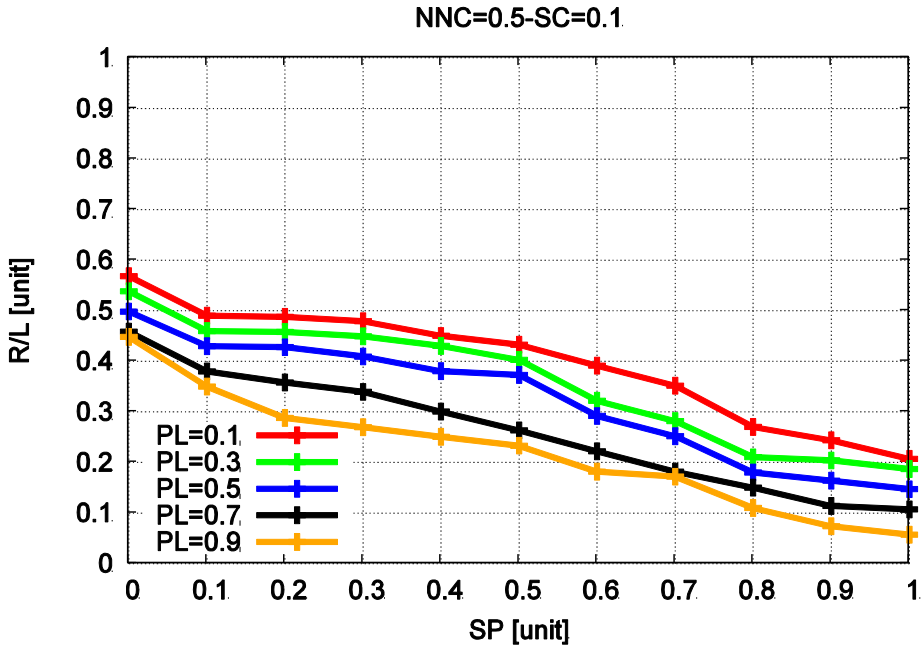
a. NNC = 0.1, SC = 0.1



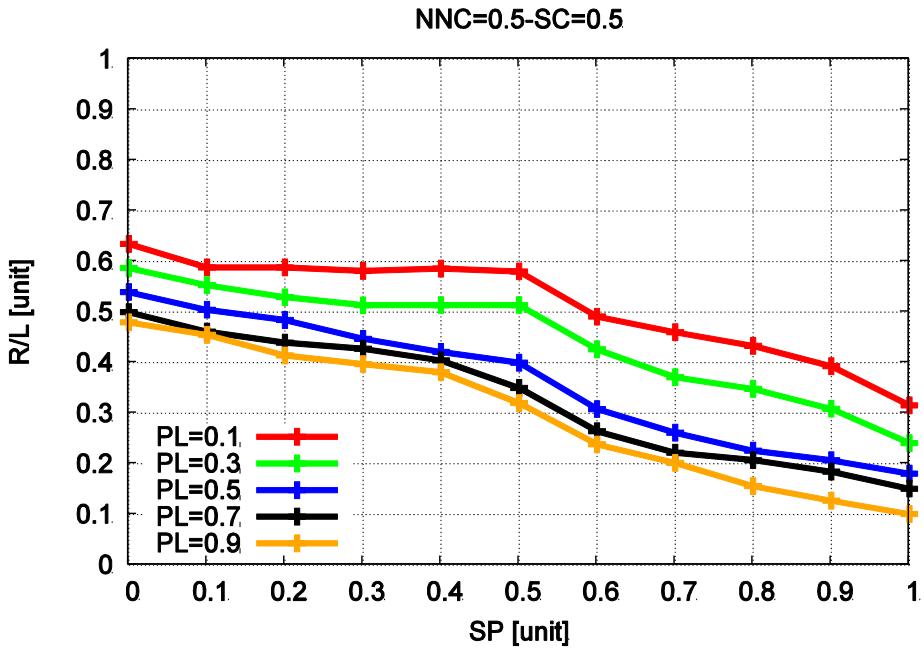
b. NNC = 0.1, SC = 0.5



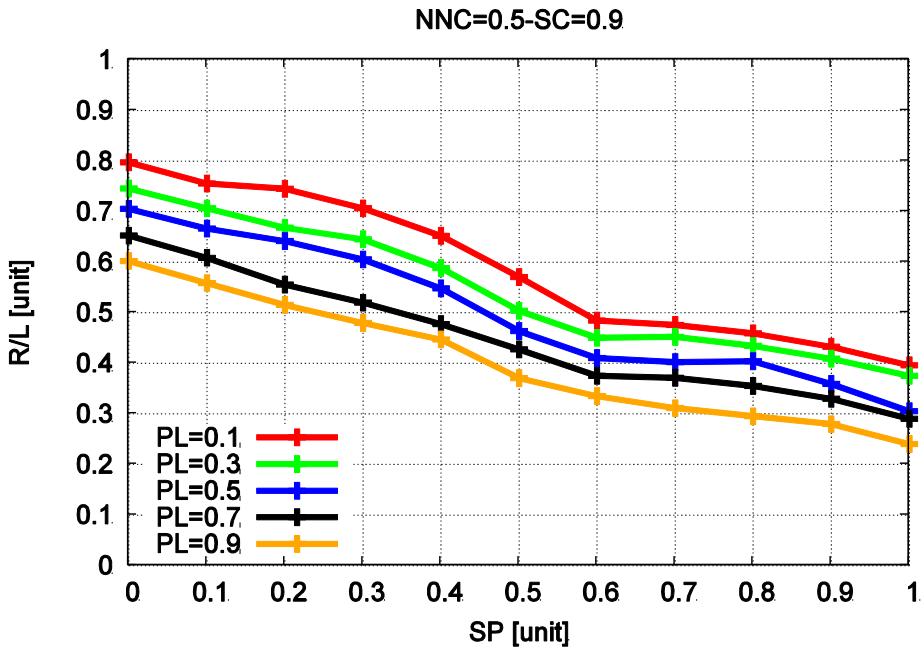
c. NNC = 0.1, SC = 0.9



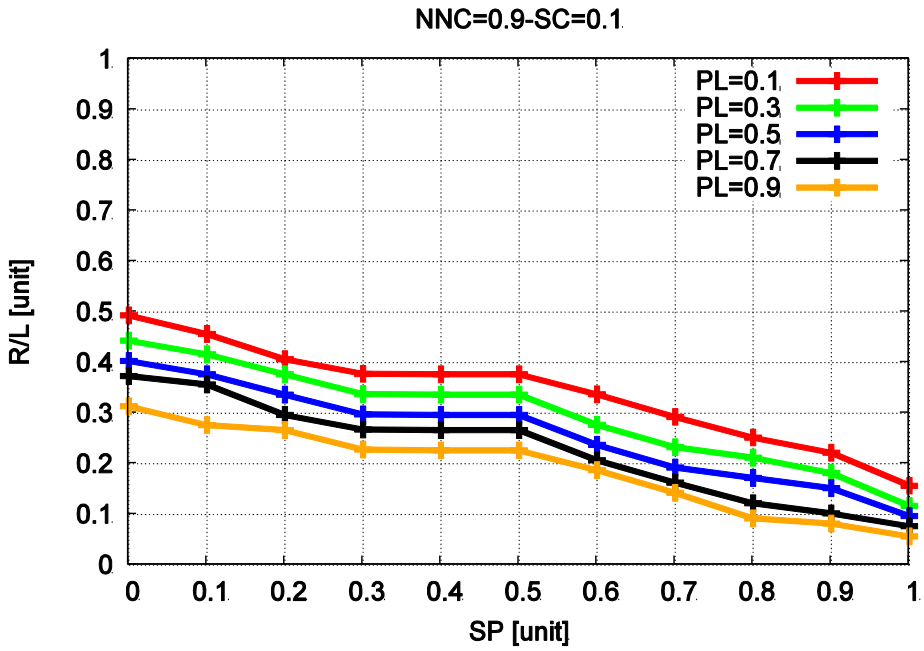
d. NNC = 0.5, SC = 0.1



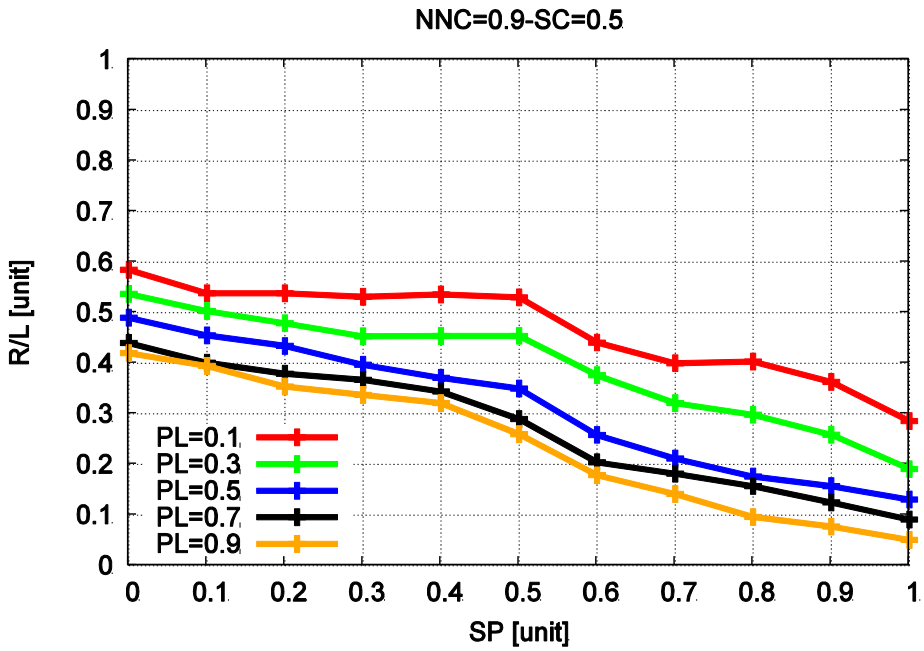
e. NNC = 0.5, SC = 0.5



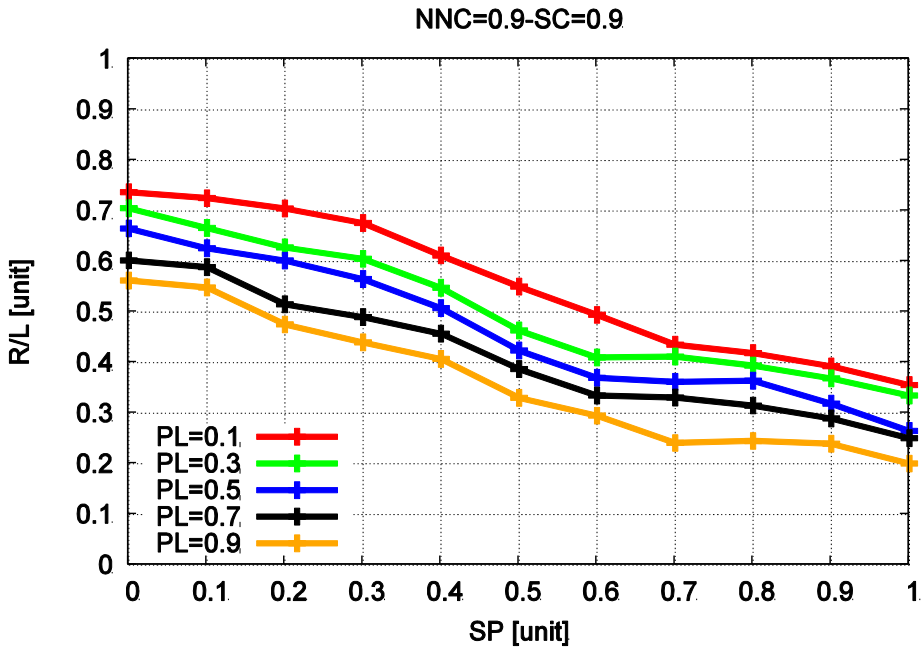
f. NNC = 0.5, SC = 0.9



g. NNC = 0.9, SC = 0.1



h. NNC = 0.9, SC = 0.5



i. NNC = 0.9, SC = 0.9

Figura 5.7. Lidhja ndërmjet parametrave të hyrjes dhe daljes për sistemin F2SMC2

Pra siç vihet re nga rezultatet e simulimeve për F2SMC2 duke zgjedhur nyjet me vlerë të lartë sigurie nyjet janë më të besueshme dhe performanca e rrjetit përmirësohet.

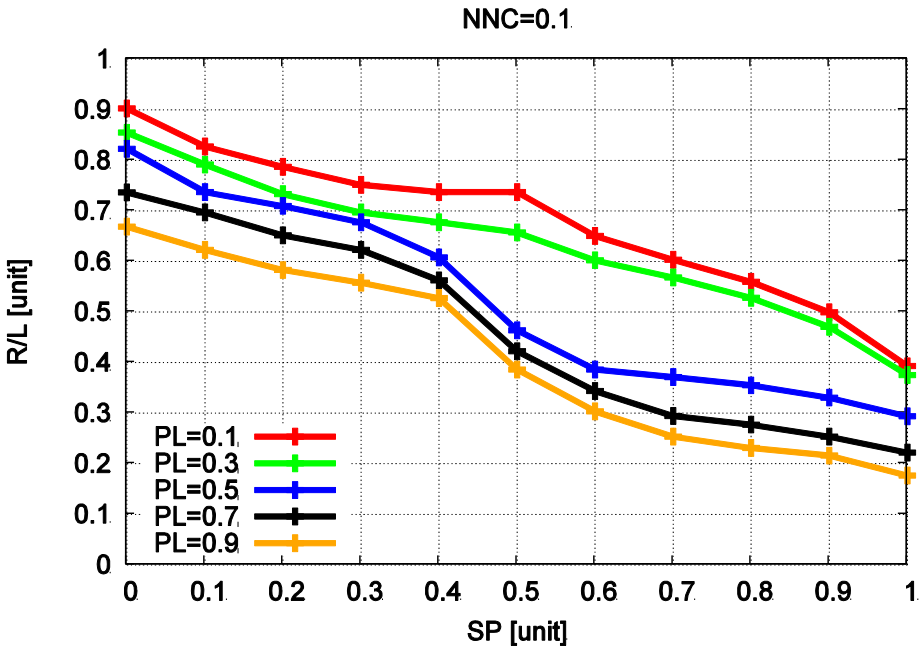
5.7 Krahasimi i dy sistemeve të propozuar

Në sistemin F2SMC1 konsiderojmë tre parametra në hyrje ndërsa në sistemin F2SMC2 kemi konsideruar katër parametra në hyrje, pra shtojmë dhe sigurinë e nyjes tek sistemi i dytë. Konsiderojmë në F2SMC1 numrin e nyjeve konstant dhe vëmë re nga simulimet që me rritjen e fuqisë së shpenzuar dalja zvogëlohet. Gjithashtu kur rritet numri i nyjeve nga 0.1 në 0.9 dalja zvogëlohet. Në F2SMC1 konsiderojmë humbjen e paketave si parametrin e besueshmërisë dhe vëmë re se me uljen e humbjes së paketave nyjet janë më të besueshme. [55], [56]

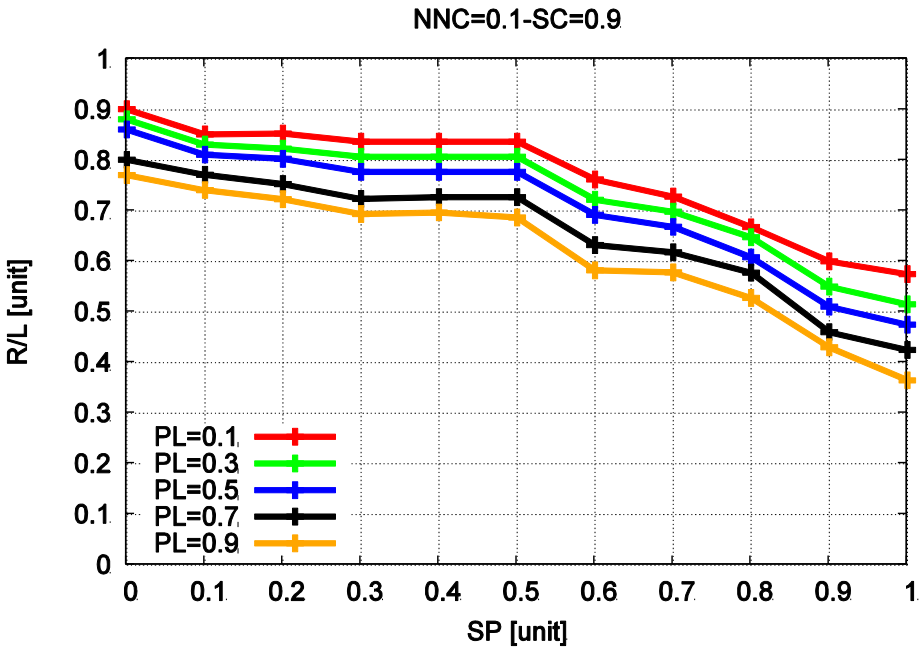
Në sistemin F2SMC2 konsiderojmë numrin e nyjeve dhe sigurinë konstante. Vëmë re se me rritjen e vlerës së sigurisë së nyjeve dalja rritet, që do të thotë nyja është e

besueshme. Siguria si parametër hyrje jep një kontribut të rëndësishëm në daljen e sistemit. Nga simulimet vihet re që me rrtijen e numrit të nyjeve dalja zvogëlohet, por rënia e daljes është më e vogël se në rastin e sistemit F2SMC1.

Vihet re që me rritjen e numrit të nyjeve dalja zvogëlohet, pra nyjet tentojnë të largohen nga cluster.

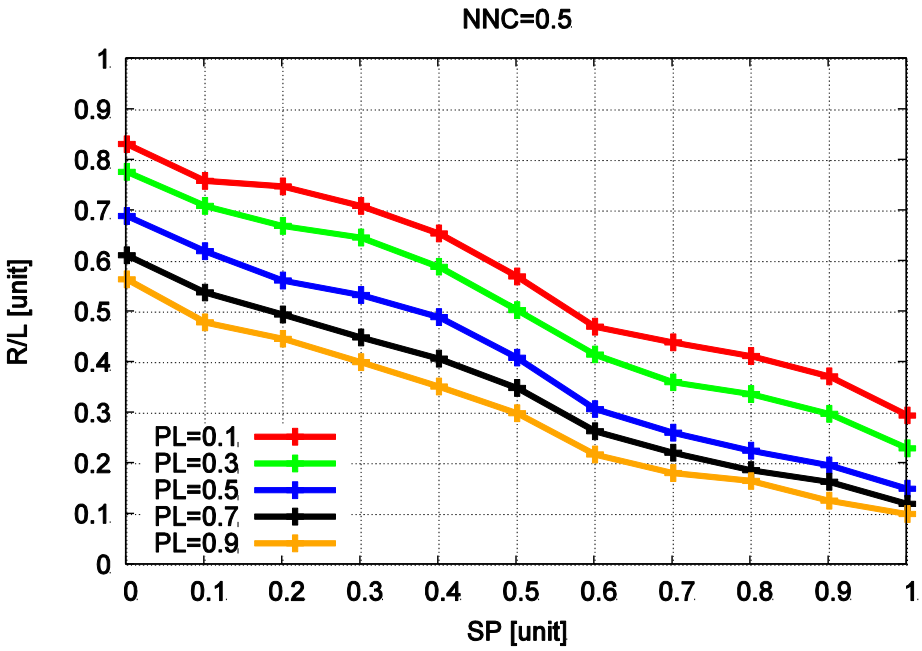


a. Dalja për sistemin F2SMC1

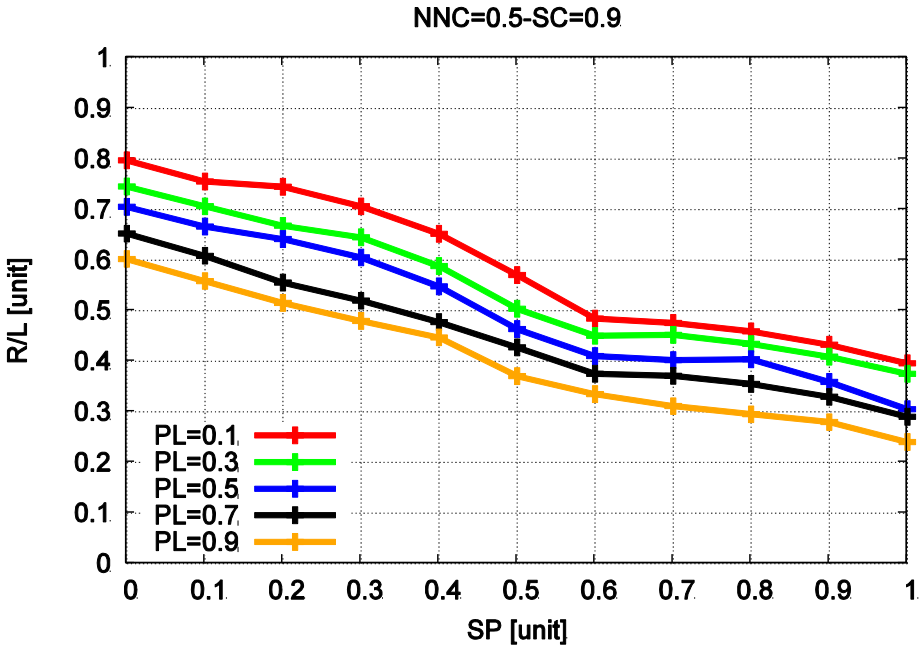


b. Dalja për sistemin F2SMC2 për NNC=0.1 njësi dhe SC=0.9 njësi

Figura 5.8. Krahasimi i dy sistemeve për NNC =0.1 njësi.

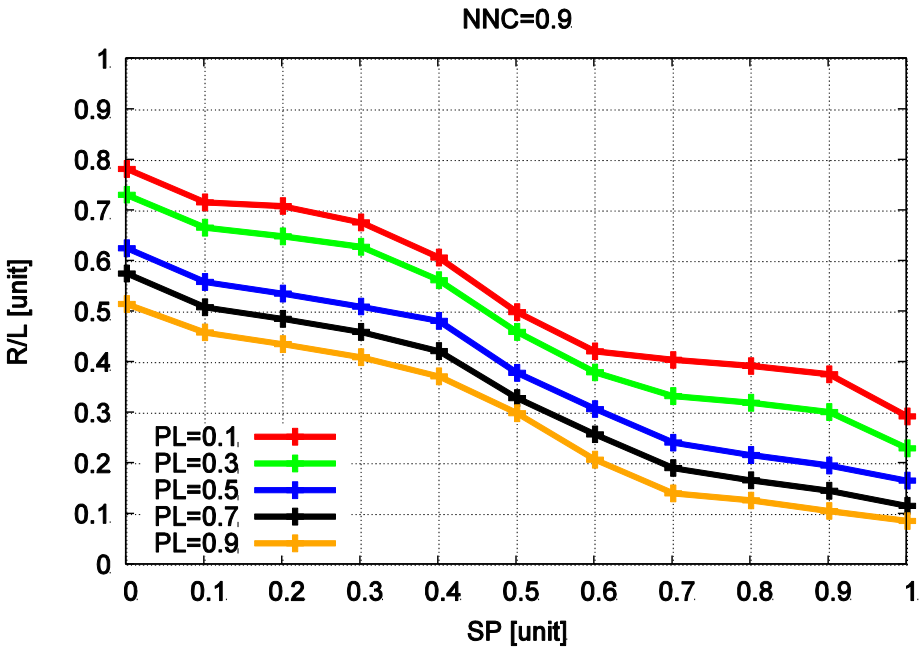


a. Dalja për sistemin F2SMC1 për NNC=0.5 njësi

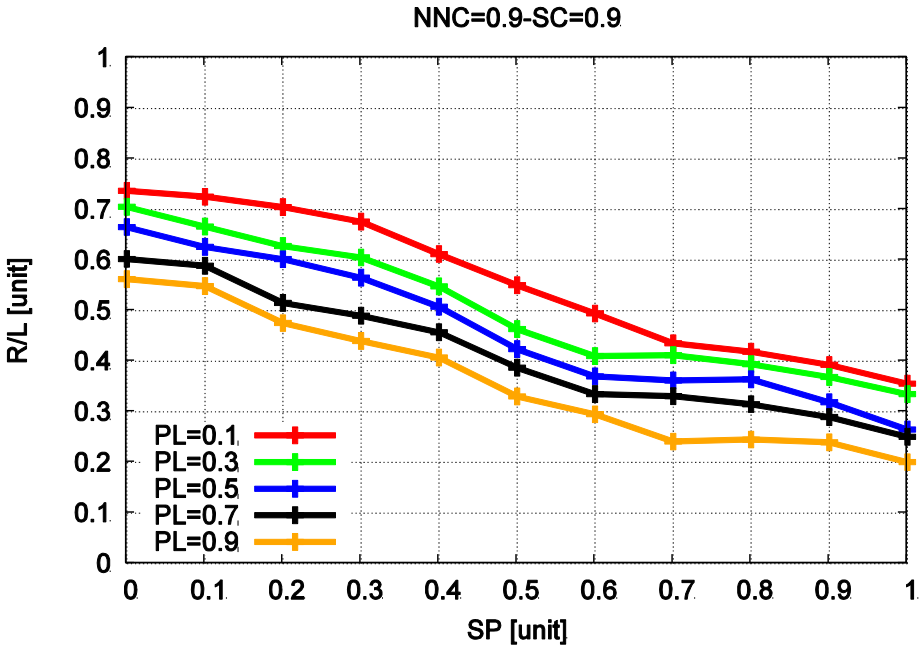


b. Dalja e sistemit F2SMC2 për NNC=0.5 njësi dhe SC=0.9

Figura 5.9. Krahasimi i dy sistemeve për NNC =0.1 njësi.



a. Dalja e sistemit F2SMC1 për NNC=0.9 njësi



b. Dalja e sistemit F2SMC2 për NNC=0.9 njësi dhe SC=0.9

Figura 5.10. Krahasimi i dy sistemeve për NNC =0.1 njësi

Vihet re nga figurat 5.8, 5.9, 5.10 që për të njëjtin numër nyjesh në cluster kur shtohet dhe parametri i sigurisë së nyjes në hyrje dalja rritet, pra clusteri bëhet më i besueshëm.

Sistemi F2SMC2 është më kompleks se F2SMC1 por është më i besueshëm se F2SMC1. Duke marrë parasysh përmirësimin e besueshmërisë së nyjeve cluster si dhe performancën më të mirë të F2SMC2 mund të themi se sistemi F2SMC2 është më i mirë se F2SMC1.

PËRFUNDIME

1. Përfundime të punimit

Rrjetat MANET kanë karakteristika të përcaktuara unike që i bëjnë ato të cënueshëm nga sulme të ndryshme. Meqenëse këto rrjeta vendosen në mjedis të hapur ku të gjitha nyjet bashkë veprojnë në dërgimin e paketave në rrjet, nyjet me qëllim të keq është e vështirë të zbulohen. Ndaj është e vështirë të ndërtohet një protokoll i sigurtë krahasuar me rrjetat me tel ose ato të bazuar në infrastrukturë. Krijimi i një komunikimi të sigurtë të të dhënave në MANET është një sfidë interesante dhe e vështirë.

Në literaturë janë propozuar protokolle të shumtë sigurie, si përmirësim ose zgjerim i protokolleve egzistuese. Gjithashtu janë propozuar modele ose metoda sigurie për një rrjet specific me karakteristika të përcaktuara dhe bëhet përmirësimi i performancës së sistemit.

Në këtë punim u paraqitën dy sisteme për vlerësimin e besueshmërisë së nyjeve cluster të cilët mund të implementohen në çdo lloj rrjeti MANET të ndarë në clustera.

Sistemet vlerësojnë besueshmërinë e nyjeve heterogjene duke u bazuar në karakteristikat e tyre të ndryshme të vlerësuara më pare nga algoritme të ndryshëm.

Informacioni i mbushur me pasaktësi dhe paqartësi si dhe aftësia e fuzzy logic më modelimin gradual të karakteristikave të rrjetit bazuar dhe në eksperinecën e ekspertëve të rrjetit e bëjnë fuzzy logic mjaft të përdorshëm në shumë aplikime.

Meqenëse FLC është një metodë intuitive, tolerante me paasaktësitë në të dhëna, e lehtë për t'u kuptuar si dhe bazohet në gjuhën natyrore, rrit interesin dhe aplikueshmërinë e mëtejshme të saj.

Në këtë punim u propozuan dy sisteme të bazuar në fuzzy logic për përcaktimin dhe vlerësimin e besueshmërisë së nyjeve në cluster në MANET. Në sistemin e parë F2SMC1 u morën në konsideratë tre parametra në hyrje: numri i nyjeve në cluster, humbja e paketave dhe fuqia e shpenzuar. Duke u bazuar në këto parametra hyrje u përcaktua për çdo nyje në cluster nëse është e besueshme të mbetet në cluster apo duhet të largohet nga cluster. Nga rezultatet eksperimentale u arrit në përfundimin se sistemi i propozuar rrit besueshmërinë e rrjetit dhe përmirëson performancën e tij.

Për të rritur më tej besueshmërinë e nyjeve në cluster dhe për ta përmirësuar sistemin F2SMC1 u shtua në hyrje dhe një parametër i katërt që është siguria e nyjeve. Pra u Propozua një sistem i dytë F2SMC2 i cili është më kompleks por më i besueshëm dhe më i sigurtë se sistemi F2SMC1. Nga rezultatet eksperimentale vihet re se duke zgjedhur nyjet me vlerë të lartë sigurie clusterat janë më të sigurtë dhe si rezultat dhe rrjeti është më i sigurtë dhe i besueshëm, si dhe performanca e rrjetit përmirësohet.

2. Objektiva për të ardhmen

Në vijim të punës/kontributit të këtij punimi lindin dhe objektiva për të ardhmen si më poshte:

- Të konsiderohen në hyrje dhe parametra të tjerë për përmirësimin e mëtejshëm të sistemit
- Të rrisim numrin e simulimeve për sistemet.

LISTA E SHKURTIMEVE

CA	Certificate Authority
TC	Topology Control
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
CH	Cluster Head
IDS	Intrusion Dedection Systems
ITU	International Telecommunications Union
DAC	Disrecionale Access Control
MAC	Mandatory Access Control
RBAC	Role Based Access Control
DoS	Denial of Service
HMAC	Hash Message Authentication Code
FL	Fuzzy Logic
FC	Fuzzy Control
PID	Proportional- Integral-Derivative Controller
FLC	Fuzzy Logic Controller
FIS	Fuzzy Inference System
COA	Center of Area Method
MOM	Mean of Maximum Method
F2SMC	Fuzzy Secure System in MANET Cluster
NNC	Number of Nodes in Cluster
PL	Packet Loss
SP	Spent Power
SC	Security
R/L	Remain/Leave
PAN	Personal Area Network
LAN	Local Area Network

WLAN	Wireless Local Area Network
OLSR	Optimised Link State Routing
BATMAN	Better Aproach to Mobile Ad-Hoc Networking
DSDV	Destination-Sequenced Distance-Vector Routing
DSR	Dynamic Source Routing
AODV	Ad-Hoc on-Demand Distance-Vector
TORA	Temporally Ordered Routing Algorithm
ZRP	Zone Routing Protocol
IARP	Intrazone Routing Protocol
IERP	Interzone Routing Protocol
BRP	Boardercast Resolution Protocol
MobDHop	Mobility-Based D-Hop Clustering Algorithm
MPBC	Mobility Prediction-Based Clustering
3-hBAC	3-hop Between Adjacent Cluster Heads
KCONID	K-hop Connectivity ID Clustering Algorithm
ECEC	Enhance Topology Control Protocol
WCA	Weighted Clustering Algorithm
FWCA	Flexible Weight Based Clustering Algorithm
GPRS	General Packet Radio Service
UMTS	Universal Mobile Telecommunications System
ARAN	Authenticated Routing for Ad-Hoc Networks
ARIADNE	A Secure on-Deamand Routing Protocol for Ad-Hoc Networks
CONFIDANT	Cooperation of Nodes: Fairness in Dynamic Ad-Hoc Networks
SADOV	Secure Ad-Hoc on-Demand Distance-Vector
SPAAR	Secure Position Aided Ad-Hoc Routing
ALERT	An Anonymous Location-Based Efficient Routing Protocol
SAR	Secure Aware Ad-Hoc Routing Protocol
SEAD	Secure Efficient Distance-Vector Routing Protocol
CBTRP	A Cluster-Based Trust-Aware Routing Protocol

STACRP	A Secure Trusted Auction Oriented Clustering Routing Protocol
SCA	Secure Clustering Based Algorithm
FRD	Fuzzy Relevance Degree
FRCA	Fuzzy Relevance-Based Cluster Head Selection Algorithm

LITERATURA

[1] Edited by Xin Wang, “Mobile Ad-Hoc Networks: Protocol Design”, 2011

[2] Tirthraj Rai, “Security in Mobile ad hoc networks”, 2009

[3] Hanan M. M. Abu-Thuraia, “Secure Zone Routing Protocol in Ad-Hoc networks”, 2010

[4] Aarti, Dr. S. S. Tyagi, “Study of MANET: Characteristics, Challenges, Application and Security Attacks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X

[5] Mr. L Raja, Capt. Dr. S Santhosh Baboo, “An Overview of MANET: Applications, Attacks and Challenges”, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 408-417

[6] Tanu Preet Singh, Satinder Kaur, Vikrant Das, “Security Threats in Mobile Adhoc Network: A Review”, IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol. 2, No. 1, 2012

[7] Harjeet Kaur, Varsha Sahni, Dr. Manju Bala, “A Survey of Reactive, Proactive and Hybrid RoutingProtocols in MANET: A Review”

[8] RFC AODV (Ad-Hoc On Demand Distance Vector Routing)

[9] RFC OLSR (Optimised Link State Routing)

[10] M. Swathi, B. Pravallika, N. V. Muralidhar, “Implementing And Comparison of MANET Routing Protocols Using NS2”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014

[11] Ali Hilal Al-Bayatti, “Security Management for Mobile Ad hoc Network of Networks (MANoN)”, 2009

[12] Rehan Akbani, “Defending Against Malicious Nodes in Closed MANETs Through Packet Authentication and a Hybrid Trust Management System”, 2009

[13] Salwa Aqeel Mahdi, Mohamed Othman,Hamidah Ibrahim, Jalil Md. Desa and Jumat Sulaiman, “Protocols for Secure Routing and Transmission in Mobile Ad hoc Networks: A Review”, Journal of Computer Science 9 (5): 607-619, ISSN 1549-3636, 2013

[14] G.S. Mamatha, Dr. S.C. Sharma, “Network Layer Attacks and Defense Mechanisms in MANETS- A Survey”, International Journal of Computer Applications (0975 – 8887) Volume 9– No.9, November 2010,

[15] Niroj Kumar Pani, “A Secure Zone-Based Routing Protocol for Mobile Ad hoc Networks”, 2009

[16] Karamvir Singh, Harmanjot Singh, “Securing MANET Using Diffie Hellman Digital Signature Scheme”, International Journal For Advance Research in Engineering and Technology, Volume 2, Issue IX Sep 2014 ISSN 2320-6802

[17] Thandu Naga Srinu Padma, Tandu Ramarao, Nischala Simhadri, “AODV Routing Protocol in MANET based onCryptographic Authentication Method”, IJCSET |October 2012 | Vol 2, Issue 10, 1459-1464, ISSN:2231-0711

[18] Haiying Shen, Lianyu Zhao, “ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs”, IEEE Transaction on Mobile Computing, Vol. 12, No. 6, June 2013.

[19] Mehdi Maleknasab, Moazam Bidaki, Ali Harounabadi, “Trust-Based Clustering in Mobile Ad Hoc Networks: Challenges and Issues”, International Journal of Security and Its Applications Vol.7, No.5 (2013), pp.321-342

[20] G.Saranya, “Forming A Secure Cluster In MANET Using Frd Algorithm”, Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-3 , 2016

[21] D. N. Goswami and Anshu Chaturvedi, “Cross Layer Integrated Approach for Secured Cluster Selection in Ad Hoc Networks”, International Journal of Computer and Communication Engineering, Vol. 1, No. 3, September 2012

[22] Keshav Kumar Tiwari, Sanjay Agrawal, “A Secure Reputation-Based Clustering Algorithm for Cluster based energy optimized Mobile ad-hoc network”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X

[23] Abdelhak Bentaleb, Abdelhak Boubetra, Saad Harous, “Survey of Clustering Schemes in Mobile Ad hoc Networks”, Communications and Network, 2013, 5, 8-14.

[24] Madhvi Saxena, K. J. Mathai, “Analysis of Clustering Algorithms for Creation Of Energy Efficient Mobile Ad Hoc Network”, International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 11, November 2014. ISSN 2348 - 4853

[25] Harjeet Singh Chauhan, “Comparative Study of Clustering Based Algorithm in Mobile Ad-Hoc Network ”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-3, July 2013

[26] Inn Inn Er, Winston K.G. Seah,” Performance analysis of mobility-based d-hop (MobDHop) clustering algorithm for mobile ad hoc networks”, Computer Networks 50 (2006) 3375–3399.

[27] Wang Jin, Shu Lei, Jinsung Cho, Young-Koo Lee, Sungyoung Lee, Yonil Zhong, “A Load-balancing and Energy-aware Clustering Algorithm in Wireless Ad-hoc Networks”.

[28] Naveen Chauhan, Lalit Kumar Awasthi, Narottam Chand, Vivek Katiyar, Ankit Chugh, “A Distributed Weighted Cluster Based Routing Protocol for MANETs”, Wireless Sensor Network, 2011, 3, 54-60 doi:10.4236/wsn.2011.32006 Published Online February 2011

[29] Suchismita Chinara, Santanu Kumar Rath, “Mobility Based Clustering Algorithm and the Energy Consumption Model of Dynamic Nodes in Mobile Ad Hoc Network”, International Conference on Information Technology.

[30] Rani.V.G, Dr.M.Punithavalli, "MPBCA: Mobility Prediction Based Clustering Algorithm for MANET", Rani.V.G et al. / International Journal of Engineering and Technology (IJET)

[31] Kulbhushan Jagpreet Singh, "Fuzzy Logic Based Intrusion Detection System against Blackhole Attack on AODV in MANET",

[32] Marti, S., Giuli, T.J., Lai, K., Baker, M."Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, 2013.

[33] Nidal Nasser and Yunfeng Chen, " Enhanced Intrusion Detection System for discovering Malicious Nodes in Mobile Ad hoc Networks" Communications, 2007. ICC '07. IEEE International Conference.

[34] Varsha Himthani, Prashant Hemrajani & Sachin Sharma," Optimizing the efficiency of watchdog IDS in MANETs using selfishness information and bayesian filtering", Vol. 3, Issue 2, Mar 2014, 131-140.

[35] Shafigh, A. S. Abdollahi, K. Kassler. Andeas J, "Improving Performance Of On Demand Multicast Routing By Using Fuzzy Logic" in IEEE International Conference 2010.

[36] Morteza Romoozi and Hamideh Babaei, "A P2P Fuzzy Reputation System Based on Security Policies for Mobile Ad-Hoc Networks", *International Journal of Information and Electronics Engineering, Vol. 3, No. 5, September 2013*

[37] Arash Dana, Golnoosh Ghalavand, Azadeh Ghalavand and Fardad Farokhi, "A Reliable routing algorithm for Mobile Adhoc Networks based on fuzzy logic",

[38] Partha Sarathi Banerjee, J. Paulchoudhury, S. R. Bhadra Chaudhuri, "Fuzzy Membership Function in a Trust Based AODV for MANET", I.J. Computer Network and Information Security, 2013, 12, 27-34

[39] Introduction to Fuzzy Logic using MATLAB, S. N. Sivanandam, S. Sumathi and S. N. Deepa, Springer-Verlag Berlin Heidelberg 2007

[40] L. A. Zadeh, "Fuzzy Logic, Neural Networks, and Soft Computing", Communications ACM (92pp), pp. 77-84, March 1994.

[41] A. Kandel, "Fuzzy Expert Systems," CRC press, 1991.

[42] H.-J. Zimmermann, "Fuzzy Set Theory and Its Applications," Springer Science & Business Media, 1991.

[43] L. A. Zadeh and J. Kacprzyk, "Fuzzy Logic for the Management of Uncertainty," John Wiley & Sons, Inc., 1992.

[44] G. J. Klir and T. A. Folger, "Fuzzy Sets, Uncertainty, and Information," Prentice Hall, 1988.

[45] Ying Bai, Dali Wang "Fundamentals of Fuzzy Logic Control – Fuzzy Sets, Fuzzy Rules and Defuzzifications"

[46] Y. Liu, S. Sakamoto, K. Matsuo, M. Ikeda, L. Barolli, and F. Xhafa, "Improvement of JXTA-Overlay P2P Platform: Evaluation for Medical Application and Reliability," International Journal of Distributed Systems and Technologies (IJDST), vol. 6, no. 2, pp. 45–62, 2015.

[47] K. Matsuo, D. Elmazi, Y. Liu, S. Sakamoto, G. Mino, and L. Barolli, "FACS-MP: A Fuzzy Admission Control System with Many Priorities for Wireless Cellular Networks and Its Performance Evaluation," Journal of High Speed Networks, vol. 21, no. 1, pp. 1–14, 2015.

[48] D. Elmazi, S. Sakamoto, T. Oda, E. Kulla, E. Spaho, and L. Barolli, "Two Fuzzy-Based Systems for Selection of Actor Nodes inWireless Sensor and Actor Networks: A Comparison Study Considering Security Parameter Effect," Mobile Networks and Applications, pp. 1–12, 2016.

[49] V. Kolici, T. Inaba, A. Lala, G. Mino, S. Sakamoto, and L. Barolli, "A Fuzzy-Based CAC Scheme for Cellular Networks Considering Security," The 17th International

Conference on Network-Based Information Systems (NBiS-2014), pp. 368–373, 2014.

[50] T. Inaba, S. Sakamoto, T. Oda, M. Ikeda, and L. Barolli, “A Secure-Aware Call Admission Control Scheme for Wireless Cellular Networks Using Fuzzy Logic and Its Performance Evaluation,” Journal of Mobile Multimedia, vol. 11, no. 3&4, pp. 213–222, 2015.

[51] D. Elmazi, E. Kulla, T. Oda, E. Spaho, S. Sakamoto, and L. Barolli, “A Comparison Study of Two Fuzzy-based Systems for Selection of Actor Node in Wireless Sensor Actor Networks,” Journal of Ambient Intelligence and Humanized Computing, vol. 6, no. 5, pp. 635–645, 2015.

[52] Y. Liu, S. Sakamoto, K. Matsuo, M. Ikeda, and L. Barolli, “Improving Reliability of JXTA-Overlay Platform: Evaluation for E-learning and Trustworthiness,” Journal of Mobile Multimedia, vol. 11, no. 2, pp. 34–50, 2015.

[53] Mirjeta Alinci, Takaaki Inaba, Donald Elmazi, Evjola Spaho, Vladi Kolici and Leonard Barolli, “Clustering Algorithms in MANETs: A review”, CISIS 2015, 978-1-4799-8870-9/15 $31.00 © 2015 IEEE DOI 10.1109/CISIS.2015.47

[54] Mirjeta Alinci, Takaaki Inaba, Donald Elmazi, Evjola Spaho, Vladi Kolici and Leonard Barolli “Improving Reliability of Cluster Nodes in MANETs: A Fuzzy-Based Approach”, AINA 2016.

[55] Mirjeta Alinci, Takaaki Inaba, Donald Elmazi, Evjola Spaho, Vladi Kolici and Leonard Barolli “A Fuzzy-based System for Improving Node Security in MANET Clusters”, CISIS 2016, 978-1-5090-0987-9/16 $31.00 © 2016 IEEE DOI 10.1109/CISIS.2016.54

[56] Mirjeta Alinci, Takaaki Inaba, Donald Elmazi, Evjola Spaho, Vladi Kolici and Leonard Barolli, “Improving Node Security in MANET Clusters: A Comparison Study of Two Fuzzy-based Systems”, NBiS 2016.

[57] Mirjeta Alinci, Vladi Koliçi, Evjola Spaho, " A fuzzy based system for improving reliability in MANET ", The International Journal of Science, Innovation and New Technology, ISSN 2223-2257.

[58] Mirjeta Alinci, Vladi Koliçi, Algenti Lala, "Propozimi i një sistemi bazuar në logjikën Fuzzy për vlerësimin e besueshmërisë së nyjeve cluster në MANET", Buletini i Shkencave Teknike të UPT, 2016.

[59] Mirjeta Alinci, Takaaki Inaba, Donald Elmazi, Evjola Spaho, Vladi Kolici, Leonard Barolli, "A Comparison of Two Fuzzy-based Systems Considering Node Security in MANET Clusters", The International Journal of Grid and Utility Computing (IJGUC)

[60] Ezmerina Kotobelli, Elma Zanaj, Mirjeta Alinci, Edra Bumçi, Mario Banushi "The Study of Interference between UMTS and Wi-Fi in Indoor Environments", The international Journal of Advanced Computer Science and Applications (IJACSA), Vol 6, No. 7, 2015.

[61] Mirjeta Alinci, Elma Zanaj, Ezmerina Kotobelli, " Effect of Black hole attack on mobile Ad-hoc network performance on environmental monitoring", 28 May – 2 June 2012, BALWOIS 2012 (Fifth International Scientific Conference on Water, Climate and Environement)

[62] Mirjeta Alinci (Kovaçi), Elma Zanaj, Ezmerina Kotobelli, "Perfomance analysis of the attacks in MANET", 8-9 June 2012, Information Systems and Technology Innovation: their application in Economy, ISBN: 978-9995-6377-8-1.

[63] Elma Zanaj, Ermal Elbasani, Mirjeta Alinci, Ezmerina Kotobelli, Blerina Zanaj, "Application of the localization algorithms in WSN", 2-5 September 2014, UPEC2014 (International Universities Power Engineering Conference), 978-1-4799-6557-1/14/$31.00 © 2014 IEEE

[64] Ezmerina Kotobelli, Elma Zanaj, Mirjeta Alinci, " Data Management in WSNs by a light cost algorithm", 8-9 June 2012, Information Systems and Technology Innovation: their application in Economy, ISBN: 978-9995-6377-8-1

[65] Ezmerina Kotobelli, Elma Zanaj, Mirjeta Alinci, “An Improved Algorithm for Efficient Data Management in Wireless Sensor Networks”, 28 May – 2 June 2012, BALWOIS 2012 (Fifth International Scientific Conference on Water, Climate and Environement)

[66] Elma Zanaj, Indrit Enesi, Deivis Disha, Mirjeta Alinci, Ezmerina Kotobelli, “Measuring the Perfomance of DSR Protocol Configurable in a Real Environment”, 28 May – 2 June 2012, BALWOIS 2012 (Fifth International Scientific Conference on Water, Climate and Environement)

[67] Elma Zanaj, Indrit Enesi, Arjan Bici, Ezmerina Kotobelli, Mirjeta Alinci, “Real Applications in Ad-Hoc Networks”, 28 May – 2 June 2012, BALWOIS 2012 (Fifth International Scientific Conference on Water, Climate and Environement)