Universitatea "Politehnica" din Bucureşti Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

Optimizarea rutarii bazate pe vectori distantă în reţele ad-hoc

Proiect de diplomă

prezentat ca cerinţă parţială pentru obţinerea titlului de Inginer în domeniul Calculatoare şi Tehnologia Informaţiei programul de studii de licenţă Ingineria Informaţiei

Conducător ştiinţific
Conf. dr. ing. Ştefan STĂNCESCU

Absolvent
Pîrvu Sorin-Nicolae

Universitatea "Politehnica" din Bucureşti
Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

Departamentul Electronică Aplicată şi Ingineria Informaţiei

Aprobat Director de Departament :

Prof. Dr. Ing. Sever Paşca

TEMA PROIECTULUI DE DIPLOMĂ
a studentului
Pîrvu V. Sorin Nicolae,grupa 442A

1. Titlul temei:Optimizarea rutarii bazate pe vectori distantă în reţele ad-hoc

2. Contribuţia practică, originală a studentului va consta în (*în afara* părţii de documentare): Comparaţia privind performaţele protocoalelor de rutare în reţele ad-hoc; modificarea unui algoritm bazat pe vectori distanţă în vedere optimizării rutării; elaborarea de scenarii de simulare şi comparaţii de performanţă privind algoritmul modificat; folosind simulatoare uzuale NS(Network Simulator), Cisco Packet Tracer,OPNET etc.

3. Proiectul se bazează pe cunoştinţe dobîndite în principal la următoarele discipline: Arhitecturi de Reţea şi Internet, Reţele de Calculatoare, Sisteme de Operare

4. Realizarea practică/ proiectul rămân în proprietatea: *UPB/* Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

5. Proprietatea intelectuală asupra proiectului aparţine: *UPB/* Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

6. Locul de desfăşurare a activităţii: *UPB/* Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

7. Data eliberării temei: 27 Noiembrie 2012

CONDUCĂTOR LUCRARE:

Conf. Dr. Ing Ştefan Stăncescu

STUDENT:

Pîrvu Sorin Nicolae

Declaraţie de onestitate academică

Prin prezenta declar că lucrarea cu titlul *Optimizarea rutarii bazate pe vectori distantă în reţele ad-hoc*, prezentată în cadrul Facultăţii de Electronică, Telecomunicaţii şi Tehnologia Informaţiei a Universităţii "Politehnica" din Bucureşti ca cerinţă parţială pentru obţinerea titlului de *Inginer* în domeniul domeniul Calculatoare şi Tehnologia Informaţiei programul de studii de licenţă Ingineria Informaţiei este scrisă de mine şi nu a mai fost prezentată niciodată la o facultate sau instituţie de învăţământ superior din ţară sau străinătate.

Declar că toate sursele utilizate, inclusiv cele de pe Internet, sunt indicate în lucrare, ca referinţe bibliografice. Fragmentele de text din alte surse, reproduse exact, chiar şi în traducere proprie din altă limbă, sunt scrise între ghilimele şi fac referinţă la sursă. Reformularea în cuvinte proprii a textelor scrise de către alţi autori face referinţă la sursă. Înţeleg că plagiatul constituie infracţiune şi se sancţionează conform legilor în vigoare.

Declar că toate rezultatele simulărilor, experimentelor şi măsurătorilor pe care le prezint ca fiind făcute de mine, precum şi metodele prin care au fost obţinute, sunt reale şi provin din respectivele simulări, experimente şi măsurători. Înţeleg că falsificarea datelor şi rezultatelor constituie fraudă şi se sancţionează conform regulamentelor în vigoare.

Bucureşti, ***15.09.2013*** **Absolvent Pîrvu Sorin-Nicolae**

_____

(semnătura în original)

Lista acronimelor

ACK = Acknowledgement
AODV = Ad Hoc Ondemand Distance Vector - Rutare cu Vector de Distanţă la Cerere.
AOMDV = Ad Hoc Ondemand Multiple Distance Vector - Rutare cu Vectori de Distanţă Multipli la Cerere.
ARP = Address Resolution Protocol – Protocol de rezolvarea a adreselor
CBR = Continuous Bit Rate
CSMA/CA = Carrier sense multiple access/ collision avoidance – Access multiplu cu detecţie de purtătoare/ Evitarea coliziunilor
CTS = Clear To Send- Liber pentru transmisie
DCF = Distributed Coordination Function
DSDV = Destination-Sequenced Distance-Vector - Vector Distanţă cu Destinaţie Dinamică Ordonată
DSR = Dynamic Source Routing – Rutare dinamică folosind sursa
DSSS = Direct Sequence Spread Spectrum
EIGRP = Enhanced Interior Gateway Routing Protocol
ETSI = European Telecommunications Standards Institute
FTP = File Transfer Protocol
HTTP = Hyper-Text Transfer Protocol
ICMP = Internet Control Message Protocol – protocolul mesajelor de control din Internet
IMEP = Internet MANET Encapsulation Protocol
IEEE = Institute of Electrical and Electronics Engineers
IP = Internet Protocol – Protocol Internet
ISM = Industrie, Stiinta, Medicina
LAN = Local Area Network
MAC = Medium Access Control
MANET = Mobile Ad-hoc NETworks
OFDM = Orthogonal Frecvency Division Multiplexing
OSI = Open Systems Interconnection
OSPF = Open Shortest Path First
OPNET = Optimized Network Engineering Tool
PDA = Personal Digital Assistant
PCF = Point Coordination Fonction
RIP = Routing Information Protocol
RERR = Route Error – mesaj de eroare de rută
RREQ = Route Request - mesaj de cerere de rută
RREP = Route Reply – mesaj de răspuns la rută
RTS = Ready To Send- Gata pentru transmisie
TCP = Transport Control Protocol – Protocol de control al transportului
TTL = TTL- Timp de viaţă
TORA = Temporally Ordered Routing Algorithm
UNII = Unlicensed National Information Infrastructure
UDP =User Datagram Protocol - Protocol cu Datagrame Utilizator
WMN = Wireless Mesh NETworks
WSN = Wireless Sensor NETworks
ZRP = ZoneRouting Protocol
ZHLS = Zone based Hierarhical Link State routing

Introducere:

În aceasta lucrares se reprezintă un studiu de performanţă al rutării în cadrul reţelelor ad hoc.

Reţelele ad hoc reprezintă reţele dinamice, mobile, care nu necesită o arhitectură fixă sau procese de configurare. Implementarea unor astfel de reţele reprezintă o direcţie deosebită în care se îndreaptă noile generaţii de comunicaţie. Aplicaţiile sunt diverse şi se bazează foarte mult pe proprietăţile de mobilitate şi auto organizare. Cum intersul pentru astfel de reţele creşte pe zi ce trece, este nevoie şi de o creştere de performanţă . Performanţa unei reţele ad hoc este dată în principal de modul în care protocoalele de rutare organizează comunicarea. Este nevoie de protocoale de rutare dinamice, rapide, care să facă faţă cu succes schimbărilor dese de topologie.

Obiectivele acestei lucrări constau în a analiza eficienţa protocoalelor de rutare standard, create special pentru astfel de medii mobile, folosind indicatori de performanţă uzuali precum throughput sau timpul mediu de întârziere a pachetelor pentru diverse scenarii şi totodată de a oferi soluţia de rutare cea mai potivită fiecărui scenariu în parte. Scenariile propuse au fost create în scopul de a simula, pe cât posibil, evenimente reale şi aplicabile unor astfel de reţele. Fiecare scenariu urmăreşte să pună în evidenţă anumite aspecte ale rutării şi ale comportamentului protocoalelor de rutare în reţele ad hoc.

Capitolul 1. Reţele ad hoc

Noțiunea de rețea ad-hoc utilizată în această lucrare reprezintă o rețea wireless dinamica fără o infrastructură fixă, formată din noduri mobile care utilizează interfețe wireless pentru a trimite pachete de date. Rețele mobile ad-hoc au fost în centrul multor cercetări recente si eforturi de dezvoltare vizand în principal aplicații militare datorită mobilității acestora.

1.1 Tipuri de Retele ad-hoc

Rețelele ad-hoc pot fi clasificate în mai multe tipuri în functie de aplicațiile în care acestea sunt folosite: [1]

- Retele ad-hoc mobile (MANET - Mobile Ad-hoc NETworks) .
- Reţele wireless de tip plasă (WMN - Wireless Mesh NETworks).
- Reţele wireless de senzori (WSN - Wireless Sensor NETworks) .

1.1.1 Rețelele ad-hoc mobile (MANET)

O rețea mobila ad-hoc (MANET) este un tip descentralizat de reţea formată din dispozitive mobile care se deplasează independent în orice direcţie, prin urmare îşi va schimba frecvent conexiunile cu celelalte dispozitive din rețea. Rețelele ad-hoc mobile pot fi implementate cu diverse tehnologii wireless cum ar fi standardul 802.11/WiFi , transmisia celulară sau prin satelit.

Principala provocare în construirea unei MANET este echiparea fiecărui dispozitiv astfel încât să menţină în permanență informațiile necesare pentru a ruta traficul în mod corespunzător. Aceste rețele pot funcționa separat sau poate fi conectate la Internet.

Reţelele ad-hoc moblile (MANET) se împart în trei categorii: [2]

- Reţele ad-hoc Vehiculare (VANET): sunt utilizate pentru comunicarea între vehicule şi echipamentele instalate la marginea drumului.
- Rețele ad-hoc Vehiculare Inteligente (InVANET): sunt un fel de inteligență artificială, care ajută vehiculele să se comporte în mod inteligent în timpul ,coliziunilor vehicul-vehicul, accidente etc.
- Reţele ad-hoc mobile bazate pe Internet (iMANET): acest tip de reţea face legătura dintre dispozitivele mobile din cadrul uni MANET şi Internet.

1.1.2 Rețelele wireless de tip plasă (WMN)

O rețea wireless de tip plasă (WMN) este o rețea de comunicații formată din noduri radio organizate într-o topologie de tip plasă (mesh).

O rețea plasă este de încredere și oferă redundanță. Când un nod nu mai poate funcționa, restul de noduri pot comunica încă între ele, în mod direct sau prin noduri intermediare. Rețelele wireless de tip plasă pot fi implementate cu diverse tehnologii wireless , respectiv 802.11 , 802.15 , 802.16 sau tehnologiile celulare. [3]

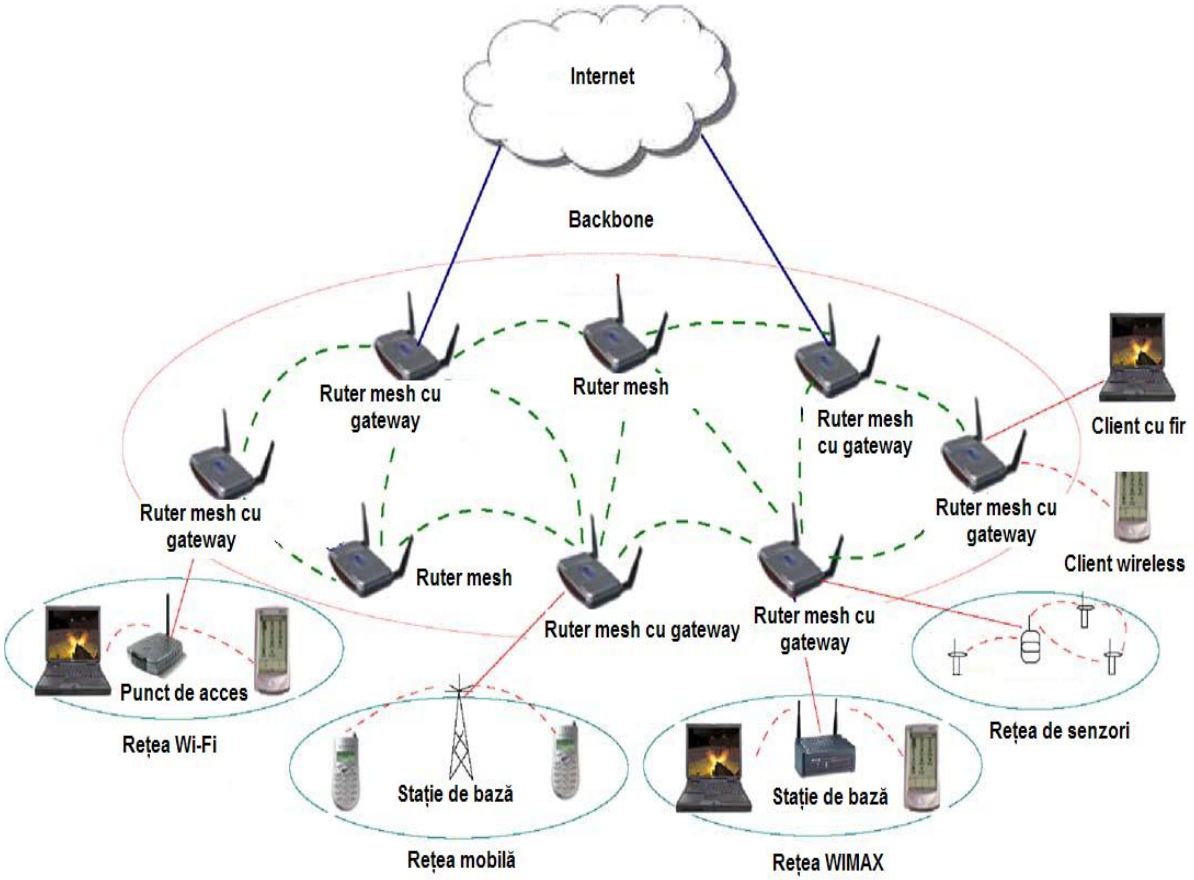

Figura 1.1 Rețelea wireless de tip plasă [3]

1.1.3 Reţele wireless de senzori (WSN)

O rețea de senzori wireless (WSN) este alcătuită din senzori autonomi distribuiţi spaţial cu scopul de a monitoriza condițiile fizice sau de mediu, cum ar fi temperatura, sunetul, presiunea, umiditatea etc. și pentru a transfera datele rezultate prin intermediul reţelei la o locație principală. Cele mai multe rețele de senzori moderne sunt bidirecţionale, cu rolul de a permite controlul activității senzorilor. Dezvoltarea de rețele de senzori wireless a fost motivată de aplicaţiile militare, cum ar fi supravegherea câmpului de luptă; astăzi aceste rețele sunt folosite în multe aplicații industriale și de consum, cum ar fi monitorizarea stării de sănătate.

În informatică și telecomunicații, rețele de senzori wireless sunt un domeniu de cercetare activ cu numeroase ateliere de lucru și conferințe organizate în fiecare an . [4]

1.2 Standardele IEEE 802.11

Standardul IEEE 802.11 defineşte două moduri de acces la un mediu. Este vorba despre:

- *Distributed Coordination Function* (DCF) este un protocol de gestiune cu acces multiplu cu detectarea coliziunilor (Carrier Sense Multiple Access with Collision Avoidance / CSMA/CĂ) cu scopul de a maximiza rata medie de transmitere a pachetelor.
- *Point Coordination Fonction* (PCF) este un mod în care staţiile de bază au ca rol gestionarea accesului la canal în zona de acoperire pentru mobilele care le sunt ataşate.

În reţelele ad hoc, nu există staţii de bază fixe, modul DCF fiind cel utilizat. [5]

Principiul de funcţionare al modului DCF constă în ascultarea mediului pentru a vedea dacă o altă staţie va emite. Staţia trebuie să se asigure că mediul este liber pentru o anumită durata înainte de a emite. Dacă mediul este liber în acest timp, sursa poate începe emiterea datelor, iar în caz contrar transmisia este amânată pentru o perioadă de timp aleasa aleatoriu, după care staţia va reîncerca să trasmita din. Totuşi, dacă cel puţin două staţii emit simultan, poate apărea o coliziune care din păcate nu poate fi detectată de staţia emitentă. Pentru această situaţie se utilizează o "confirmare" (ACK-acknowledgement) cu scopul de a informa staţia emitentă că a fost recepţionat cu succes cadrul.

Staţia emitentă trimite mai întâi un mesaj scurt RTS (Request To Send) conţinând destinaţia şi durata transmisiei. Celelalte staţii ştiu astfel că mediul va fi ocupat în timpul acesta. Destinaţia, dacă mediul este liber, va permite sursei să transmită, emiţând un mesaj scurt CTS (Clear To Send) care indică sursei că poate începe să emită datele fără riscul unei coliziuni.

În loc de un singur standard IEEE 802.11b, există un întreg alfabet de variante wireless din care utilizatorii pot alege : 802.11a, 802.11b, 802.11g şi 802.11h , 802.11n etc. [6]

1.2.2 Tehnologia

Reţelele wireless se împart în două clase importante, factorul decisiv fiind frecvenţa de bandă. Tehnologiile moştenite folosesc banda de 2.4 GHz, în timp ce variantele ulterioare folosesc banda mai lată, de 5 GHz. Prima clasă include standardul The Institute of Electrical and Electronics Engineers (IEEE) 802.11b (11 Mbps) şi succesorul său, 802.11g (54 Mbps). Această primă clasă este, în prezent, cea mai frecventă opţiune. Pe de altă parte, 802.11a şi 802.11h, ambele putând să obţină o rata nominală de 54 Mbps, operează în banda de 5 GHz.

802.11b a fost ratificat de IEEE în 1999 şi este, probabil, cel mai popular protocol de reţea wireless utilizat în prezent. Utilizează tipul de modulaţie DSSS (Direct Sequence Spread Spectrum). Operează în banda de frecvenţe ISM (Industrie, Ştiinţă, Medicină); nu sunt necesare licenţe atât timp cât se utilizează aparatura standardizată. Limitările sunt: puterea la ieşire de până la 1 Watt, iar modulaţiile numai de tipul celor care au dispersia spectrului cuprinsă între 2,412 şi 2,484 GHz. Are o viteză maximă de 11 Mbps cu viteze utilizate în prezent de aproximativ 5 Mbps. [7]

802.11g a fost ratificat de IEEE în 2003. În ciuda startului întârziat, acest protocol este, în prezent, de facto protocolul standard în reţelele wireless, deoarece este implementat practic pe toate calculatoarele care au placă wireless şi pe majoritatea celorlalte dispozitive portabile. Foloseşte aceeaşi subbanda de frecvenţe din banda ISM ca şi 802.11b, dar foloseşte tipul de modulaţie OFDM (Orthogonal Frecvency Division Multiplexing). Viteza maximă de transfer a datelor este de 54 Mbps, cu implementări practice la 25 Mbps. [8]

802.11a a fost ratificat de IEEE în 16 septembrie 1999. Utilizează tipul de modulaţie OFDM. Are o viteză maximă de 54 Mbps cu implementări de până la 27 Mbps. Operează în banda ISM între 5,745 şi 5,805 GHz şi în banda UNII (Unlicensed Naţional Information Infrastructure) între 5,170 şi 5,320 GHz. Aceasta îl face incompatibil cu 802.11b sau 802.11g. Frecventei utilizate mai mari îi corespunde o bătaie mai mică la aceeaşi putere de ieşire şi, cu toate că în subgamele utilizate spectrul de frecvente este mai liber în comparaţie cu cel din jurul frecvenţei de 2,4 GHz, în unele zone din lume folosirea acestor frecvente nu este legală. Utilizarea unui echipament bazat pe acest protocol în exterior se poate face numai după consultarea autorităţilor locale. De aceea, echipamentele cu protocolul 802.11a, cu toate că sunt ieftine, nu sunt nici pe departe la fel de populare ca cele cu 802.11b/g. [9]

802.11h, care este numită în SUA o "problemă de compatibilitate în Europa", este varianta europeană a standardului american. Cele mai importante funcţionalităţi ale acesteia sunt selectarea dinamică a frecvenţei şi puterea variabilă a transmiţătorului, pe care European Telecommunications Standards Institute (ETSI) o mandatează pentru piaţa europeană pentru a se asigura că sistemele au o putere a transmiţătorului rezonabilă. [10]

IEEE 802.11c specifică metode de wireless bridging adică metode de conectare a unor tipuri diferite de reţele prin mijloace wireless. [11]

802.11d este numit şi "*World Mode*": acest lucru se referă la diferenţele regionale din tehnologii, de exemplu cât de multe şi care canale sunt disponibile pentru utilizare şi în care regiuni ale lumii. Ca utilizator trebuie doar să numiţi tara în care doriţi să folosiţi placă WLAN şi driverul se ocupă de restul. [12]

IEEE 802.11e defineşte "*Quality-of-Service"* şi extensiile streaming pentru 802.11a/ h şi g. Scopul este de a îmbunătăţi reţelele de 54 Mbps pentru aplicaţii multimedia şi Voice over IP, adică telefonie prin reţele IP şi internet. Pentru a fi utilizată cu multimedia şi voce reţeaua să suporte ratele garantate pentru fiecare serviciu, cu întârzieri minime de propagare. [13]

802.11f descrie metodele de schimbare a standardului ("Roaming") între access point-uri, iar IAPP - Inter Access Point Protocol, se ocupă de detalii. [14]

1.3 Caracteristicile reţelelor ad-hoc

Caracteristicile reţelelor ad-hoc sunt următoarele:

- Mobilitatea: amplasarea rapidă a rețelei în zone în care nu exista o infrastructură fixa. Putem avea mobilitate individuală aleatorie, mobilitate de grup, mișcare de-a lungul rutelor pre-planificate etc. Mobilitatea poate avea un impact major asupra selecției unui sistem de rutare și poate astfel să influențeze performanţa.
- Rețea de tip multihop: este o rețea în care calea unui pachet de date trimis de la sursă parcurge un număr de noduri intemediare pentru a ajunge la destinație.
- Auto-organizare: rețeaua ad-hoc trebuie să își stabilească în mod independent parametrii proprii de configurare cum ar fi: adresarea, rutarea, poziția de identificare, controlul puterii etc. În unele cazuri, nodurile speciale (de exemplu nodurile de baza mobile) se pot coordona în mișcare astfel încât să fie distribuite dinamic în arii geografice pentru care pot furniza acoperire porţiunilor de reţea deconectate.
- Conservarea energiei: cele mai multe noduri ad-hoc (de exemplu, laptop-uri, PDA-uri, senzori etc.) au o alimentare limitată și nu au capacitatea de a-și genera singure energie (de exemplu, panouri solare). Un protocol eficient de conservare a energiei (de exemplu rutarea, descoperirea resurselor etc.) este esențial pentru longevitatea misiunii.
- Scalabilitate: în unele aplicații o rețea ad-hoc pot ajunge la câteva mii de noduri, această caracteristică dovedindu-se a fi destul de problematică. Pentru o reţea wireless scalabilitatea rețelelor este simplu de manipulat folosind o structură ierarhică.
- Securitatea: Reţelele wireless sunt relativ mai puţin sigure decât cele cablate, datorită accesului mai facil la reţea al persoanelor neautorizate aflate în zonele de acoperire ale punctelor de acces.

Există implicit în implementarea reţelelor wireless diferite bariere care formează aşa numita securitate de bază a reţelelor wireless, care împiedică accesul neintenţionat al persoanelor străine de reţea, aflate în aria de acoperire a unui punct de acces.

- Conexiune la Internet: Reţelele ad hoc pot fi configurate astfel încât să poată comunica şi cu reţele externe care au conexiune la Internet, precum reţele wireless locale, prin intermediul unor dispozitive de tranziţie. Un exemplu de astfel de dipozitiv este routerul. [11]

1.4 Aplicaţiile reteleleor ad-hoc

Particularitatea reţelei ad-hoc este că nu există nicio instalaţie fixă, ceea ce îi permite să fie o reţea rapidă şi uşor de implementat. Operaţiunile tactice precum cele de apărare, militare sau de explorare găsesc reţeaua ad-hoc ca fiind ideală. Tehnologia ad-hoc interesează de asemenea aplicarea civilă.

Putem face distincţia între:

- Serviciile de urgenţă: operaţii de căutare şi ajutare a persoanelor, cutremure, incendii, inundaţii cu scopul de înlocuire a infrastructurii cu cablu.
- Munca în colaborare sau comunicarea în întreprinderi sau clădiri : de exemplu în cadru unei reuniuni sau conferinţe.
- Bazele de date paralele.
- Aplicaţii comerciale : pentru plata electronică la distanţă (taxi) sau pentru accesul mobil la Internet său serviciu de ghidare în funcţie de poziţia utilizatorului. [15]

1.5 Probleme reţelelor ad-hoc

Într-o reţea fără fir, doua mobile pot comunica prin emitere de unde radio. Ele se partajează într-un mediu unic, însă nu pot emite în acelaşi timp. Astfel, protocolul de acces mediu a fost definit în scopul de a gestiona accesul concurent la acelaşi mediu partajat. Acest protocol face parte din familia protocoalelor de gestiune cu acces multiplu prin detectarea purtătorilor şi a coliziunilor (Carrier Sense Multiple Access with Collision Avoidance / CSMA/CĂ). El asociază un mecanism de detectare a purtătorilor înaintea transmisiei unui mecanism de aşteptare aleatorie ce permite limitarea numărului şi impactului coliziunilor. [16]

În plus, standardul defineşte un mecanism suplimentar RTS/CTS (Request To Send/Clear To Send) pentru a evita coliziunile şi problemele nodurilor ascunse.

- **Problema staţiei ascunse** apare când două staţii nu se pot recepţiona reciproc din cauza distanţei sau a obstacolelor. Luând exemplu din figura 1.2 , Nodurile A şi C se află în raza de transmisie a nodului B , dar nu se pot detecta între ele. O coliziune se poate produce când staţiile A şi C emit date simultan stiatiei B.

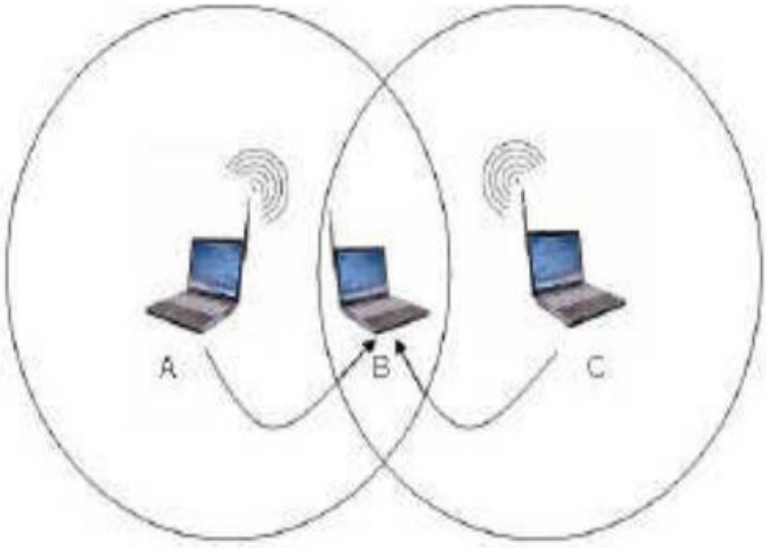

Figura 1.2 Problema staţiilor ascunse [17]

Mecanismul RTS/CTS (Request To Send/Clear To Send) permite însă rezolvarea acestei probleme. Înainte de transmiterea datelor, A vă trimite un mesaj RTS (Request To Send) lui B. Staţia B permite transmisia printr-un mesaj CTS (Clear To Send) direcţionat către A. Staţia C va aştepta încetarea transmisiei înainte de a transmite la rândul ei. [17]

- **Problema staţiei expuse** apare când o staţie vrea să stabilească o transmisie cu o a doua staţie, dar trebuie să întârzie transmisia pentru că o altă transmisie are loc între două alte staţii aflate în apropiere. Luând ca 1.3 ,staţiile A şi C pot aştepta transmisii de la B, dar staţia A nu recepţionează transimisii de la C. Presupunem şi că staţia B este pe cale să transmită date către A şi că în acelaşi timp C vrea să comunice cu D. Urmând logica CSMA/CĂ(Carrier Sense Multiple Access with Collision Avoidance), staţia C va începe prin a determina dacă mediul este liber. Din cauza comunicării între B şi A , C va găsi că mediul este ocupat şi va întârzia emiterea, deşi aceasta nu ar fi cauzat o coliziune.

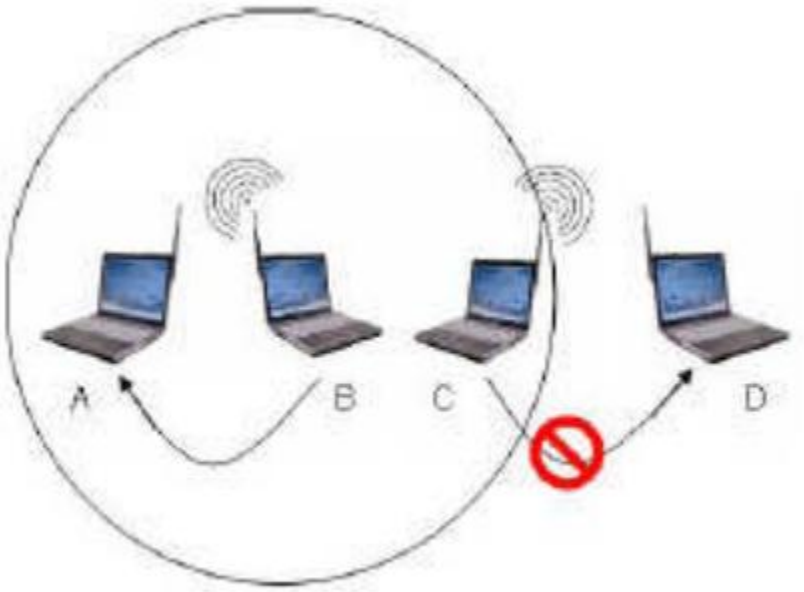

Figura 1.3 Problema staţiei expuse [17]

Capitolul 2. Protocoale de rutare bazate pe vectori distanţa în reţele ad-hoc

Dezvoltarea unui suport pentru rutare în rețele ad-hoc este una dintre cele mai importante provocări și este esențială pentru operațiunile de bază din rețea. Anumite combinaţii unice de caracteristici fac rutarea în rețele ad-hoc să fie interesantă.

În primul rând, nodurilor dintr-o rețea ad-hoc li se permite să se miște într-un mod necontrolat. Aceste noduri mobile alcătuiesc o rețea extrem de dinamică, în care se produc schimbări rapide de topologie şi din această cauză apar frecvent probleme de rutate a pachetelor. Un bun protocol de rutate pentru acest tip de rețea trebiue să se adapteze dinamic în funcţie de schimbările care pot să apară în topologie.

În al doilea rând, accesul la mediu este partajat, canalul wireless de bază oferind o lăţime de bandă mult mai mică și mai variabilă decât la rețelele cu fir. Din acest punct de vedere protocoalele de rutare trebuie să folosească eficient lăţimea de banda astfel încât o mare parte din restul lăţimii de banda trebuie să rămână disponibilă pentru comunicațiile de date reale.

În al treilea rând, nodurile din reţea folosesc baterii care au o alimentare cu energie limitată. Pentru ca nodurile să rămână și să comunice pentru perioade mai lungi, este de dorit ca un protocol de rutare să fie eficient din punct de vedere energetic.

În cadrul releleor ad-hoc protocoalele de rutare folosite se împart în trei categorii : protocoale de rutare proactive , protocoale de rutare reactive şi protocoale de rutare hibride.

- Protocoalele de rutare proactive oferă performante bune în găsire rapidă a rutei şi sunt bazate pe tabela de rutare. Avantajul acestui tip de protocol de rutate este că, după stabilirea rutelor, acestea vor fi întotdeauna disponibile şi au ca dezavantaj supraîncărcarea continuă a reţelei din cauza traficului de control.
- Protocoale de rutare reactive sunt stabilite la cerere, acestea nu îşi actualizează permanent tabela de rutare şi nu au o tabelă de rutare permanentă. Principalul dezavantaj al folosirii unui

protocol reactiv constă în inundarea reţelei cu mesaje trimise de către echipamente care nu au nici o posibilitate de a comunica cu ehipamentul solicitat.

- Protocoalele de rutare hibrite sunt o combinare de protocoale de rutare reactive şi proactive.

Interesul crescut asupra reţelelor ad-hoc a condus la crearea unor protocoale de rutare noi, schimbându-se astfel modelul în care acestea sunt împărţite în categorii. Din studiul asupra lucrării [18], protocoalele de rutare în reţelele ad-hoc au fost clasificate în felul următor:

- Scheme de rutare plate, în cadrul acestor intrând protocoalele de rutare proactive şi protocoalele de rutare reactive.
- Scheme de rutare ierarhică .
- Rutare asistata de poziţionarea geografică.

2.1 Protocoale de rutare proactive

Protocoalele de rutare proactive se mai numesc şi "table-driven" adică fiecare nod îşi poate construi singur tabela de rutare prin schimbul de informaţii intre nodurile din reţea. Acest lucru se realizează prin schimbul de mesaje de actualizare în mod regulat intre noduri pentru a menţine tabela de rutare a fiecărui nod actualizata. Apoi, când se iniţiază o transmisie nodul sursa îşi consultă propria tabela de rutare unde se afla informaţiile de rutare şi nu mai este nevoit să caute informaţii despre destinaţie , în acest fel evitându-se întârzierile cauzate de astfel de procedee.

Există două mari tipuri de protocoale de rutare folosite în Internet : bazate pe vectori distanta (de exemplu RIP,EIGRP) sau bazate pe starea legăturii (de exemplu OSPF), ambele tipuri fiind protocoale de tip proactiv. Cu toate acestea, aceste protocoale nu sunt potrivite pentru reţelele mobile ad-hoc care au resurse limitate din cauza cheltuielillor ridicate şi a convergenţei scăzute.

Algoritmul de rutare bazat pe vectorul de distanţă, denumit şi Bellman-Ford, utilizează ca şi criterii de selectare a rutei optime distanţa dintre noduri (metrică). Metrica este numărul de noduri intermediare ("hop-uri") prin care le parcurge un pachet de la o un nod sursa până la un nod destinaţie. Nodurile de reţea care utilizează acest tip de protocol gestionează informaţiile despre metrica într-o tabelă de rutare. Nodurile dintr-o reţea trimit, în mod regulat, această tabelă de rutare fiecărui nod cu care sunt conectate direct. Aceste noduri îşi actualizează propriile tabele de rutare dacă este cazul, după care la rândul lor vor trimite şi ele propriile tabele de rutare celorlalte noduri din reţea direct conectate. Aceasta face că informaţiile despre metrica să se propage în întreaga reţea, astfel încât, în final, fiecare nod să dispună de informaţii despre toate nodurile din întreaga reţea. Protocoalele de rutare bazate pe vectori distanţă sunt oarecum limitate în capacitatea de alegere a celei mai bune rute. Principalul lor avantaj constă în simplitate şi îndelungata lor folosire . În ultimii ani au fost depuse multe eforturi de a adapta algoritmul Bellman-Ford în contextul reţelelor ad-hoc , o soluţie des întâlnită în reţele ad-hoc fiind protocolul DSDV(Destination-Sequenced Distance-Vector).

Algoritmul de rutare „Vector Distanţă cu Destinaţie Dinamică Ordonată” sau DSDV (Dynamic Destination Sequenced Distance Vector) a fost unul dintre cele mai vechi protocoale dezvoltate de către C. Perkins şi P. Bhagwat pentru reţele ad-hoc. Principal obiectiv de proiectare de DSDV a fost de a dezvolta un protocol care păstrează simplitatea protocolului de rutare RIP bazându-se pe ideea algoritmului distribuit de Bellman-Ford la care au mai fost introduce unele îmbunătăţiri. [20]

La baza protocolului DSDV se aflată transferul de mesaje de control intre routerele (sau nodurile) din reţea. În acest tip de mesaje se găseşte întreaga tabela de rutare pe care o deţine fiecare nod. Traficul de control este trimis fie folosind o adresare MAC de nivel 2 sau o adresare de nivel 3 (IP).

Algoritmii bazaţi pe starea legăturilor selectează rutele optime pe baza utilizării dinamice a metodei celui mai scurt drum (Shortest Path First). Fiecare nod gestionează o "hartă" ce descrie topologia curentă a reţelei. Această hartă este actualizată regulat prin testarea posibilităţii de a accesa diferite părţi ale reţelei şi prin schimbul de informaţii cu alte rutere. Determinarea celei mai bune căi (shortest path) poate fi făcută pe baza unor metrici diferite care indică adevăratul cost al trimiterii unei datagrame pe o anumită rută. Algoritmii bazaţi pe starea conexiunii sunt mult mai puternici decât cei bazaţi pe vectori de distanţă. Ei se adaptează dinamic atunci când apar schimbări de topologie în reţea şi, de asemenea, permit selectarea rutelor pe baza unor metrici mult mai reale decât numărul de hop-uri, dar sunt mult mai complicat de instalat şi utilizează mai multe resurse pentru procesare decât cele bazate pe vectori distanţă [20].

Protocoalele de rutare proactive combina principiile algoritmilor bazaţi pe vectori distanta şi ai algoritmilor bazaţi pe starea legăturilor , încercând o adaptare a acestora în cadrul reţelelor ad-hoc.

2.2 Protocoale de rutare reactive

Protocoalele de rutare reactive se mai numesc şi protocoale de rutare la cerere ("on demand"), procesul de rutare trebuie să descopere un traseu ori de câte ori un pachet pornește de la o sursă și trebuie să ajungă la o destinație. Aici nodurile nu au o tabelă de rutare pre-construita (sau alte informaţii despre alte noduri din reţea) pe baza căreia să poată lua decizii de dirijare a infromatiilor.

Într-o reţea reactivă, procesul de descoperire al rutelor se întâmplă mai des, schimbul de mesaje se face hop cu hop, nodul sursa inundând reţeaua cu mesaje de cerere de ruta, dar acest proces necesită un trafic scăzut de control în comparație cu rutarea proactiva. Când comunicarea dintre nodul sursă şi nodul destinaţie ia sfârşit, ruta este ştearsă din tabela de rutare a dispozitivelor participante. Prin urmare, o rutare reactivă este considerată a fi mai scalabilă decât una proactiva. În plus, atunci când un nod încearcă să trimită un mesaj folosind o rutare de tip reactiv acesta trebuie să aştepte ca procestul de descoperire a căii pe unde va urma să fie trimisă informaţia să se termine, din această cauză intazierea de ansamblu va creşte. [21]

2.3 Protocoale hibride.

Protocoalele hibride combină caracteristicile protocoalelor proactive şi reactive, cu scopul principal de folosire a avantajelor acestor două tipuri de protocoale. Acest tip de reţele este împărţit în zone în interiorul cărora sunt folosite protocoale proactive iar în exterior protocoale reactive. Printre cele mai cunoscute protocoale hibride pot fi enumerate ZRP (ZoneRouting Protocol) şi ZHLS (Zone based Hierarhical Link State routing).

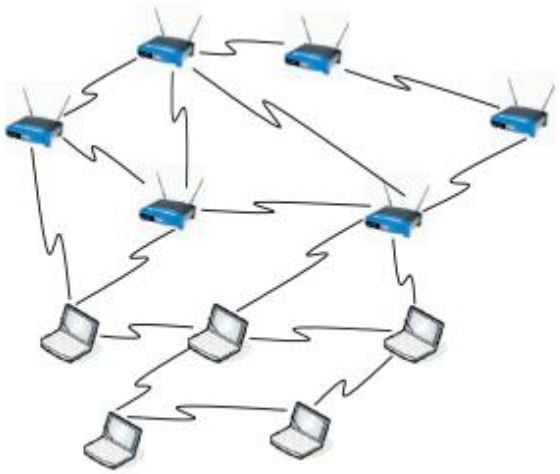

Figura 2.1 Reţele de tip hibrid. [22]

2.4 Protocolul de rutare AODV

Protocolul de rutare AODV ("Ad Hoc Ondemand Distance Vector") sau “Rutare cu Vector Distanţa la Cerere” a fost conceput pentru a îmbunătăţi performanţele protocolui de rutare DSDV şi de a reduce numărul de mesaje de broadcast şi latentă în transmisie, probleme des întâlnite la protocoalele de rutare bazate pe vectori distanta.

Protocolul de rutare AODV este un protocol de rutare reactiv, prin urmare rutele sunt determinate numai atunci când este nevoie, de exemplu procesul de rutare trebuie să descopere un traseu ori de câte ori un pachet porneşte de la o sursă și trebuie să ajungă la o destinație. Figura xyz. prezintă schimburile de mesaje ale protocolului AODV. [23]

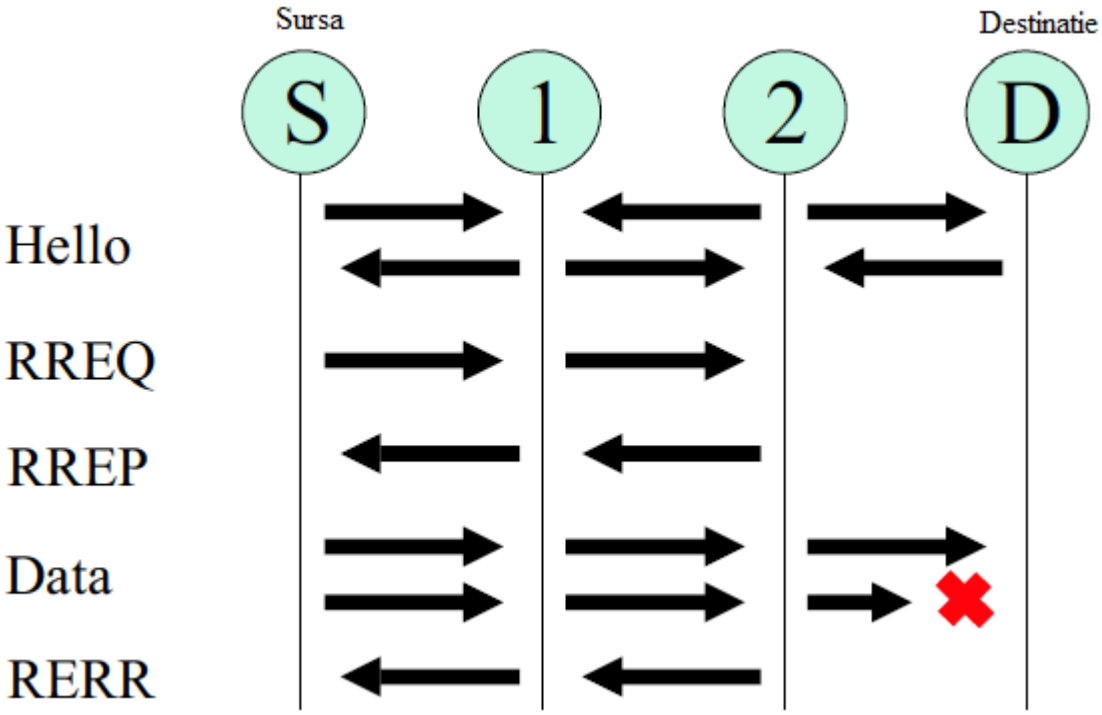

Figura 2.2 Tipurile de mesaje ale protocolului AODV [24]

Pentru a detecta şi monitoriza nodurile vecine protocolul de rutare AODV dispune de mai multe tehnici, una dintre cele mai folosite fiind schimbul de mesaje de tip "hello". Dacă se folosesc mesaje de tip "hello", fiecare nod activ va emite periodic către toţi vecinii săi un mesaj de tip "hello". În cazul în care un nod nu mai primeşte o perioadă de timp mesaje de tip "hello" de la vecinul său, atunci înseamnă că legătura s-a defectat. Tabela de rutare a nodurilor vecine este organizată să optimizeze timpul de răspuns atunci când topologia se schimbă şi să ofere un răspuns foarte rapid cererilor de stabilire a unei noi rute.

Obiectivele de bază ale algoritmului sunt următoarele [24]:

- Să trimită pachete de descoperire a rutelor numai atunci când este nevoie .
- Să facă deosebirea între managementul conectivităţii locale şi mentenanţa topologiei globale.
- Să ofere informaţii nodurilor vecine legate de schimbări în topologia locală sau starea legăturilor.

2.4.1 Descoperirea rutelor

Procesul de descoperire a rutelor se apleaza atunci când un nod dintr-o reţea ad-hoc are nevoie de o rută către o anumită destinaţie despre care nu deţine informaţii , sursa difuzează un mesaj de cerere a rutei (RREQ- ROUTE REQUEST) către toţi vecinii. Pachetul RREQ este alcătuit dintr-o adresă IP a nodului sursa, o adresă IP a nodului destinarie , un număr de secventa şi un identificator de difuzare ("broadcast_id"). Adresa IP a nodului sursă şi identificatorul de brodcast alcătuiesc un identificator unic al pachetului RREQ.

După difuzarea pachetului RREQ nodul sursa îşi setează un contor de timp şi aşteaptă un mesaj de răspuns (RREP -ROUTE REPLAY) de la nodul destinaţie. Dacă nodul sursa nu a primit un răspuns într-o anumită perioadă de timp acesta poate să presupună că nu exista o rută valida către respetiva destinaţie sau să mai încerce redifuzarea pachetului RREQ.

Când un nod primeşte un "RREQ" acesta verifica dacă a mai primit acest pachet observând adresa identificatorul de difuzare şi adresa IP a nodului sursa. Dacă pachetul a mai fost primit atunci acesta este "distrus" , dacă acesta nu a mai fost primit şi nu are o rută către respectiva destinaţie, el redifuzează respectivul pachet. Nodul creează şi o rută inversă către sursă, în care următorul hop este nodul de la care a primit mesajul, acest lucru fiind folosit pentru a avea o rută către nodul care a iniţiat căutarea, în cazul în care un pachet RREP va trebui să ajungă la sursa cererii. Aceste rute sunt temporare, în sensul că sunt păstrate valide mult mai puţin decât o rută normală . Când un mesaj RREQ ajunge la destinaţie sau la un nod care cunoaşte o rută validă către destinaţie, un mesaj RREP este creat şi trimis ca unicast către sursa cererii. Pe măsură ce pachetul trece prin nodurile intermediare, o rută către destinaţie este creată, iar când mesajul a ajuns la nodul sursă, avem deja o rută contruită . [15]

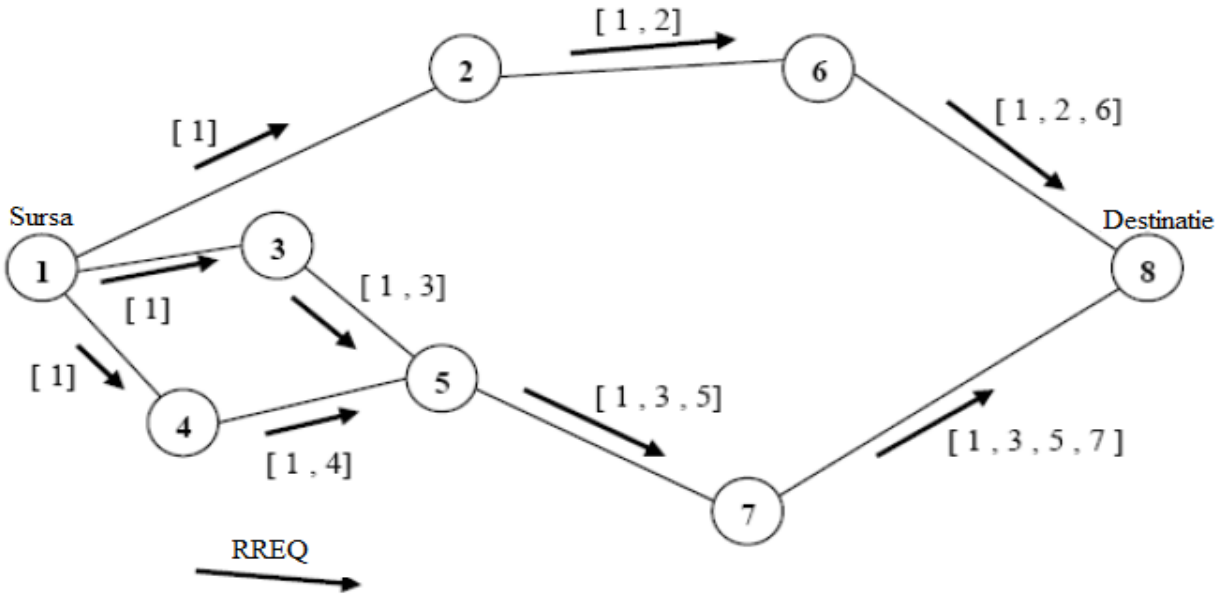

Figura 2.3 Propagarea pachetului RREQ [15]

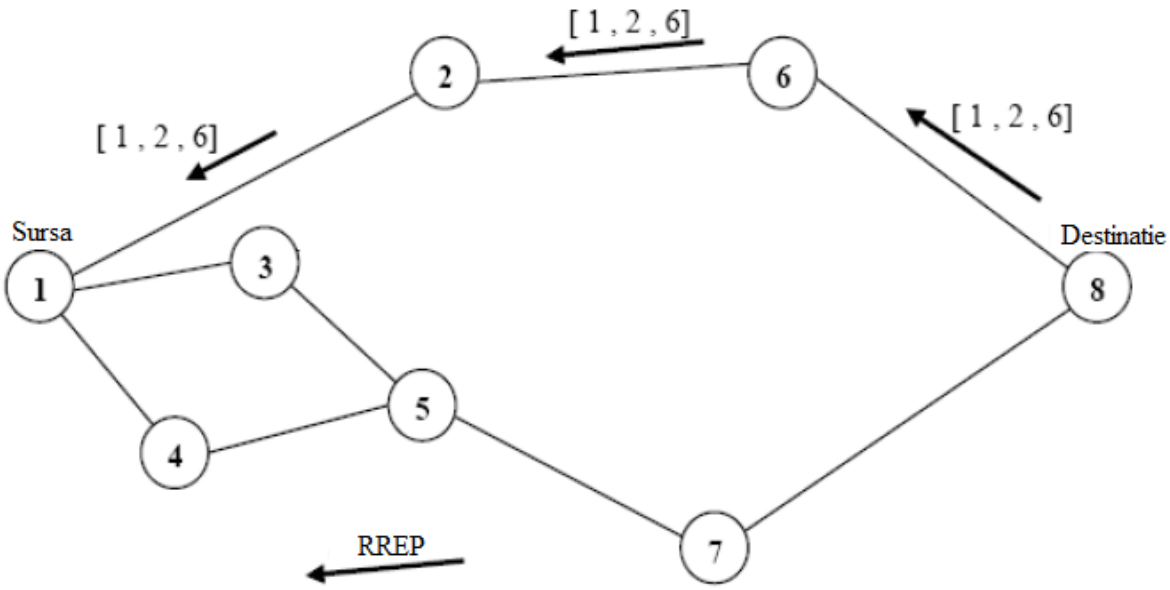

Figura 2.4 Propagarea pachetului RREP [15]

2.4.1.1 Formatul mesajelor Route Request (RREQ)

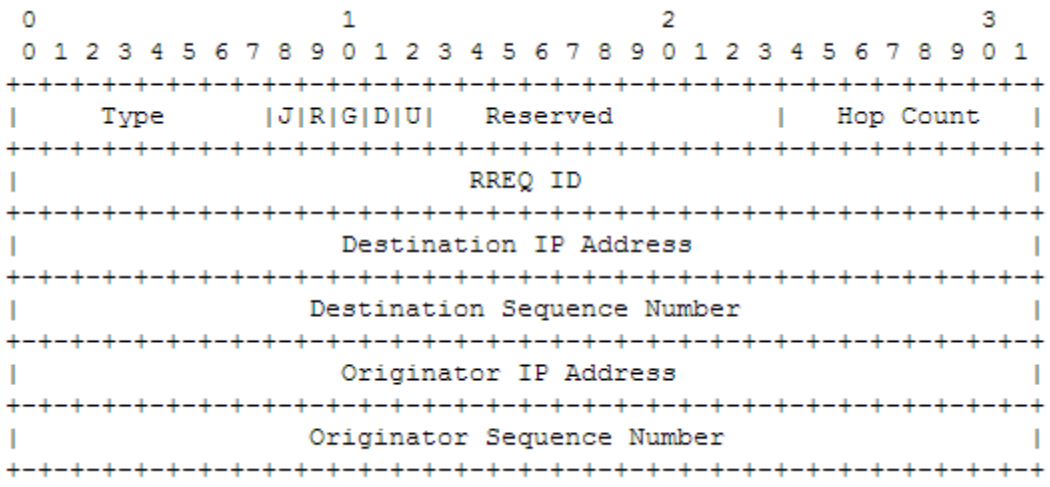

Figura 2.5 Formatul mesajelor Route Request (RREQ) [25]

Formatul mesajelor RREQ este ilustrat în figură 1.8 şi conţine următoarele câmpuri:[25]

- Tip : valoarea lui este setată cu unu , folosit pentru mesaje de tipul Route Request
- J : fanionul "Join" , este rezervat pentru comunicarea multicast.
- R : fanionul "Repair" , este rezervat pentru comunicarea multicast.
- G : fanionul Gratuit pentru Route Relay , spune când un mesaj Route Request gratuit trebuie trimis prin unicast către adresa IP destinaţie.
- D : fanionul destinaţie , indică faptul că numai destinaţia trebuie să răspundă la mesajul RREQ.

- U : număr de secventa necunoscută , indică faptul că numărul de secventa al destinaţiei este necunoscut.
- Rezervat : este trimis cu valoare zero şi este ignorat la recepţie.
- Numărul de hopuri : indica numărul de hopuri de la adresa IP sursa până la nodul care procesează acest pachet.
- RREQ ID : reprezintă un număr de secventa unic care identifică pachetele RREQ.
- Adresa IP a destinaţiei : indica adresa IP a destinaţiei pentru o rută dorită.
- Numărul de secventa al destinaţiei: indica cel mai recent număr de secventa primit într-o anumită perioadă de timp de către sursa acelui pachet către acea destinaţie.
- Adresa IP sursa : indica adresa IP a nodului care a trimis un pachet RREQ.
- Numărul de secventa al sursei : indica numărul de seventa actual care este trimis emitatotului pachetului RREQ

2.4.1.2 Formatul mesajului Route Replay (RREP)

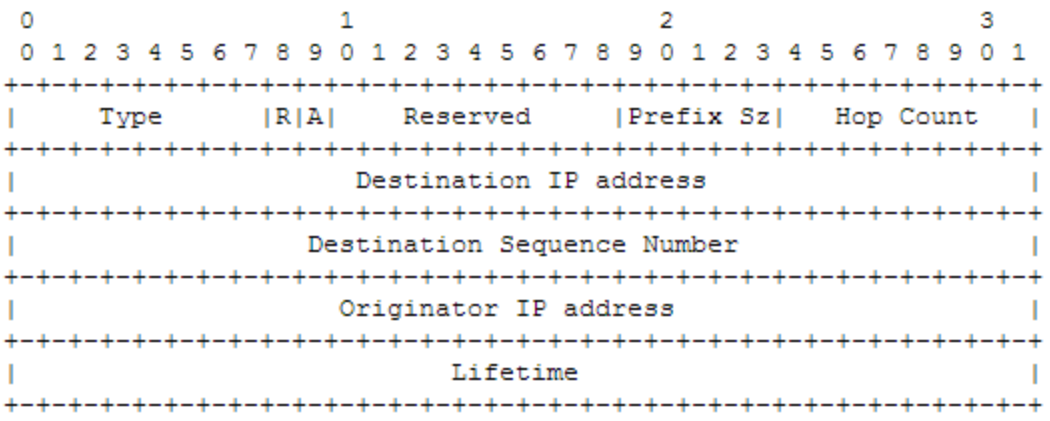

Figura 2.6 Formatul pachetelor Route Replay(RREP) [25]

Formatul mesajelor RREP este ilustrat în figură de mai sus şi conţine următoarele câmpuri:[25]

- Tip : valoarea lui este setată cu doi , folosit pentru mesaje de tipul Route Replay.
- R : fanionul "Repair" , este rezervat pentru comunicarea multicast.
- A: indică faptul că o confirmare este necesară.
- Rezervat : este trimis cu valoare zero şi este ignorat la recepţie.
- Dimensiunea prefixului : dacă nu este setat pe zero , atunci cei 5 biţi ai prefixului indică faptul că următorul nod poate fi utilizat de celelalte nodurile cu acelaşi prefix de rutare ca adresa IP destinaţie.
- Numărul de hopuri : indica numărul de hopuri de la adresa IP sursa până la nodul care procesează acest pachet.
- Adresa IP a destinaţiei : indica adresa IP a destinaţiei pentru o rută dorită.
- Numărul de secventa al destinaţiei: indica cel mai recent număr de secventa primit într-o anumită perioadă de timp de către sursa acelui pachet către acea destinaţie.
- Adresa IP sursa : indica adresa IP a nodului care a trimis un pachet RREQ.
- Durata de viaţă: timpul în milisecunde pentru care nodurile care recepţionează pachetul RREP şi consideră ruta ca fiind validă.

2.4.1.3 Formatul mesajelor Route Error (RERR).

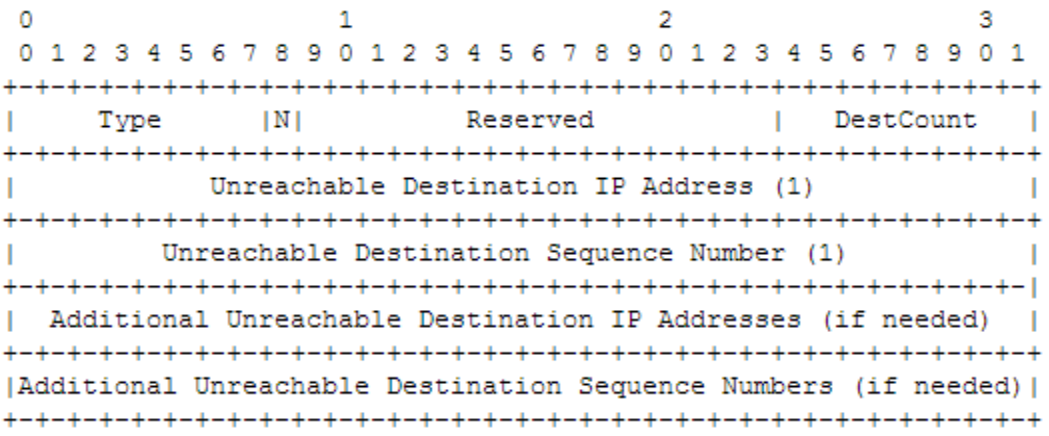

Figura 2.7 Formatul pachetelor Route Error (RERR). [25]

Formatul mesajelor RREP este ilustrat în figură 1.10 şi conţine următoarele câmpuri [25] :

- Tip : valoarea lui este setată cu trei , folosit pentru mesaje de tipul Route Error.
- Rezervat : este trimis cu valoare zero şi este ignorat la recepţie.
- N : flagul No Delete, setat atunci când un nod a realizat o reparare locală a unei legături, iar nodurile din upstream nu trebuie să şteargă această rută;
- Destinaţie IP indisponibila : atunci când o legarura este întreruptă adresa IP devine indisponibilă.
- Numărul de secventa al destinaţiei indisponibile : numărul de secvenţă din tabela de rutare pentru destinaţia listat în câmpul anterior.
- Contor Destinaţii : numărul de destinaţii indisponibile care se găseşte în pachet, trebuie să fie minim 1;

2.4.2 Mentenanţa rutelor

În momentul în care un nod are o rută către un nod vecin şi nu mai este valida , nodul care a detectat acest fapt va şterge din tabela lui de rutare ruta invalidă şi va trimite un pachet ROUTE ERROR (RERR) către toţi vecinii săi , nodurile care primesc un astfel de pachet vor trimite şi ele mai departe pachetul în reţea pentru că toate nodurile afectate să afle despre întrerupere.

Mesajul de eroare (RERR) permite protocolului AODV să se adapteze rutele atunci când apar schimbări în topologie. Ori de câte ori un nod primește un pachet RERR se uită la tabela de rutare și elimină toate rutele care conțin nodurile invalide.

În figură 1.11 sunt ilustrate circumstanțele în care un nod poate să difuzeze un pachet RERR către vecinii săi.În primul scenariu nodul primește un pachet de date care se presupune că trebuie să îl transmită mai departe , dar aceasta nu are un traseu până la destinație. Problemă reală nu este faptul că nodul nu are un traseu, problema este că un alt nod crede că traseul corect către destinație este prin acel nod.În al doilea scenariu nodul primește un pachet RERR care produce cel puțin o rută din tabela sa de rutare să fie invalidă. Dacă se întâmplă acest lucru , nodul va trimite apoi un pachet RERR cu toate nodurile noi care vor fi indisponibile.

În al treilea scenariu nodul detectează că nu poate comunica cu unul din vecinii săi. Când se întâmplă acest lucru acesta cauta în tabela sa de rutare rutele care are au următorul hop vecinul său și le marchează ca invalide. Apoi, acesta trimite un pachet RERR cu vecinul său și cu rutele invalide.[26]

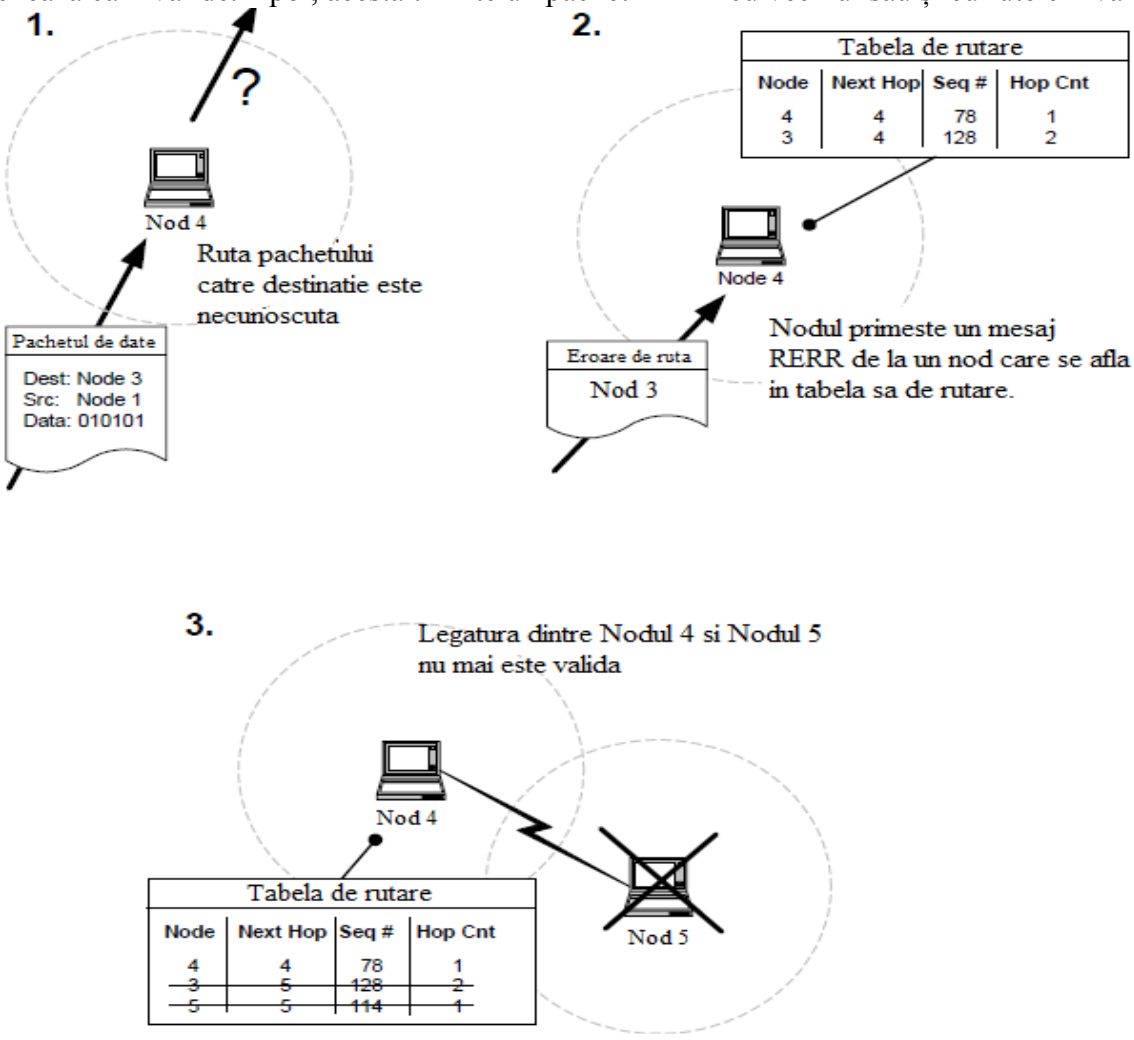

Figura 2.8 Scenarii [26]

2.4.3 Tabela de rutare

Pentru fiecare intrare din tabela de rutare AODV păstrează următoareleinformaţii:[25]

- Adresa IP a destinaţiei.
- Numărul de secvenţă al destinaţiei.
- Numărul de hopuri până la destinaţie.
- Următorul hop : vecinul care a fost desemnat pentru transmiterea pachetelor către respectiva destinaţie;
- Durata de viaţă : durata de timp pentru care ruta rămâne validă.
- Lista vecinilor activi : vecinii care folosesc acea rută la acel moment.

2.5 Protocolul de rutare TORA - Temporally Ordered Routing Algoritm

Algoritmul de Rutare Ordonat Temporal sau TORA a fost conceput în principal pentru a minimiza efectul schimbărilor de topologie care sunt frecvente în reţelele ad hoc. Algoritmul se adaptează la mobilitatea acestor medii prin stocarea de cai multiple către aceeaşi destinaţie, ceea ce face ca multe din schimbările de topologie să aibă un impact minor asupra rutării.

Un concept ce stă la baza design-ului său este acela că mesajele de control implică în general un număr mic de noduri. Salvarea cailor între o pereche (sursa, destinaţie) dată, nu se efecueaza într-o manieră permanentă. Căile sunt create şi stocate după nevoie, aşa cum este cazul tuturor protocoalele din această categorie. Optimizarea drumurilor are o importanţă secundară, căile lungi pot fi utilizate în scopul evitării declanşării unui nou proces de descoperire de noi rute.

TORA garantează că nicio rută nu prezintă bucle (bucle temporare s-ar putea totuşi forma), şi în general asigură mai multe rute pentru o pereche sursă-destinaţie. Acest protocol furnizează doar mecanismul de rutare, şi depinde de IMEP (Internet MANET Encapsulation Protocol) pentru alte funcţii. TORA poate fi separat în trei funcţii principale: crearea traseelor, menţinerea legăturilor , şi ştergerea legăturilor. Crearea rutelor se bazează pe asignarea de direcţii legăturilor, într-o reţea unidirecţională (sau sub-reţea unidirecţională), construind un graf aciclic direcţionat (DAG) cu destinaţia ca rădăcină.

TORA asociază un grad fiecărui nod din reţea. Toate mesajele în reţea circulă de la un nod cu rang mai mare către un nod cu rang mai mic. Rutele sunt descoperite flosind pachete de tip Query sau Update. Când un nod fără legături inferioare necesită o legătură către destinaţie, acesta va difuza un pachet Query. Pachetul QRY va circula în reţea până când va ajunge la un nod ce are o rută către destinaţie, sau chiar la destinaţie. Acel nod va difuza apoi un pachet Update ce conţine gradul nodului. Orice nod primeşte acest pachet îşi va seta gradul la o valoare mai mare decât a nodului de la care provine pachetul. Nodul va difuza apoi propriul pachet UPD. Procedura va conduce la crearea unui număr de legături directe sursă-destinaţie.

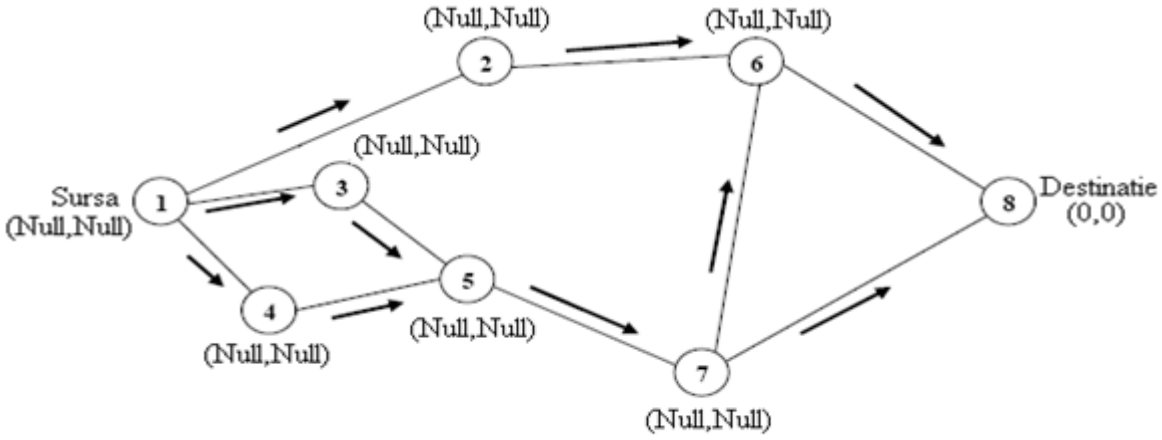

Figura 2.9 Propagarea pachetului QRY [27]

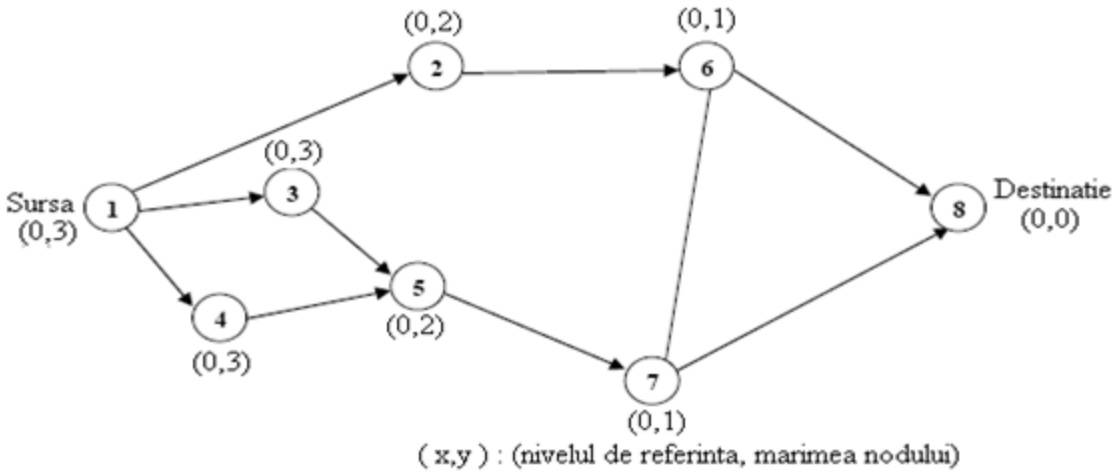

Figura 2.10 Marimile nodurilor după receptionarea pachetului UPD [27]

IMEP (Internet MANET Encapsulation Protocol) este un protocol conceput să suporte operarea mai multor protocoale în cadrul reţelelor ad-hoc. Ideea ar fi să existe un protocol comun general de care toate protocoalele de rutare să se poată folosi. Acesta încorporează mai multe mecanisme comune de care un protocol de nivel superior ar putea avea nevoie. Dintre acestea:

- Sesizarea stării legăturii
- Agregarea şi încapsularea mesajelor de control
- Fiabilitatea difuzării
- Proceduri de securitate prin autentificarea inter-router

IMEP furnizează deasemenea o arhitectură pentru identificarea routere-lor în cadrul reţelelor MANET, identificarea interfeţei şi adresare. Scopul acestui protocol este acela de a îmbunătăţi per total performanţele prin reducerea numărului de mesaje de control şi punerea unei funcţionalităţi comune într-un protocol unificat, generic folosit în cadrul tuturor protocoalelor de rutare de nivel superior. Dintre protocoalele prezentate doar TORA foloseşte IMEP. IMEP generează o supraîncărcare semnificativă în principal datorită mecanismului de descoperire a vecinilor care trimite cel puţin un mesaj ―hello pe secundă, dar şi datorită fiabilităţii pe care o oferă în ceea ce priveşte livrarea pachetelor. [27]

2.6 Protocolul de rutare DSR.

Protocolul DSR (Dynamic source routing) se bazează pe utilizarea tehnicii de rutare prin sursă. În această tehnică sursa determină secvenţa completă de noduri prin intermediul cărora pachetele de date vor fi trimise. Înainte de a trimite pachetul de date către un alt nod, emiţătorul difuzează un pachet RREQ(Request Route). Dacă operaţia de descoperire a traseului este reuşită, emiţătorul va primi un pachet RREP(Response Route) care conţine o secvenţă de noduri prin care se poate ajunge la destinaţie. Pachetul RREQ conţine un câmp de înregistrare a traseelor, în care va fi acumulată secvenţa de noduri vizitate în timpul propagării interogării în reţea. Utilizarea tehnicii de rutare prin sursă permite trimiterea de pachete de date fără ca nodurile de tranzit să aibă nevoie să păstreze informaţiile de actualizare.

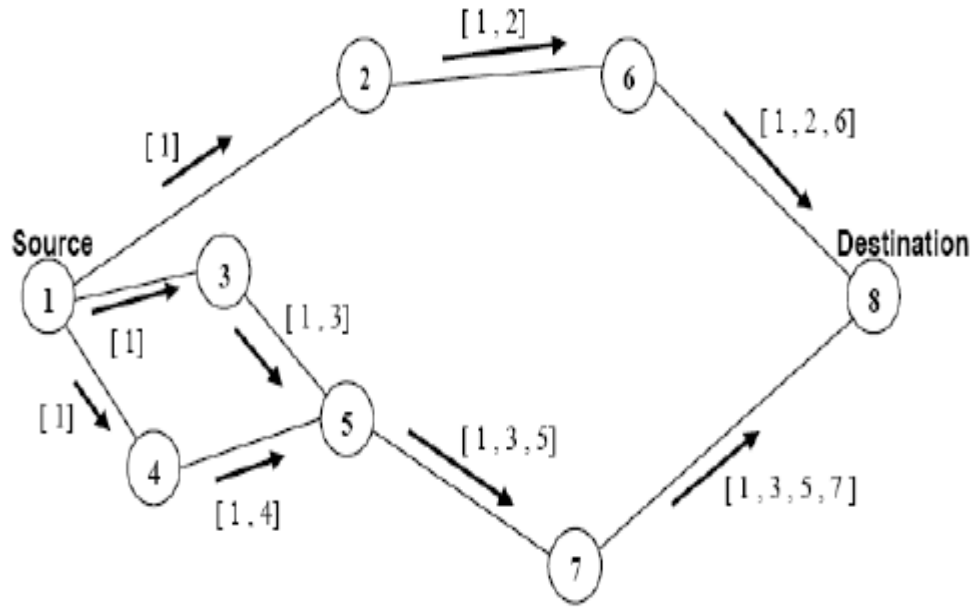

Figura 2.11 Pachet de descoperire a traseului

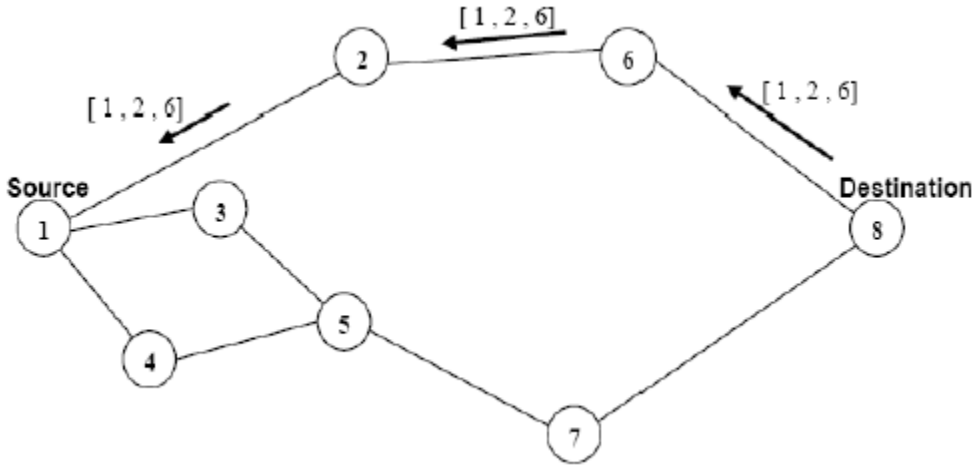

Figura 2.12 Reîntoarcerea de la destinaţie.

Formatul mesajelor Route Request (RREQ)

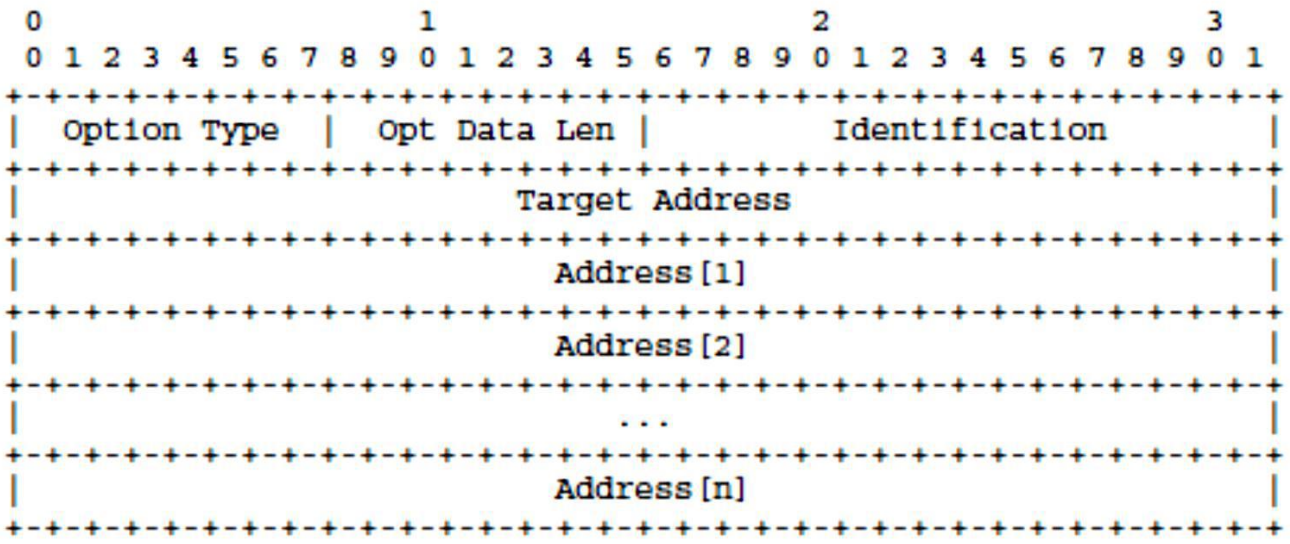

Figura 2.13 Formatul mesajelor Route Request (RREQ). [28]

Formatul mesajelor Route Request (RREQ) este alcatuit din :

- Tipul opţiunii: valoarea câmpului este setat cu 1, pentru pachete de tip Route Request.
- Opt Data Len: lungimea pachetului RREQ.
- Identificator: valoare unică generată de dispozitivul care a emis cererea de rută.
- Adresa [ ]: adresa IPv4 a nodului i înregistrat în opţiunea Route Request. [28]

Formatul mesajelor Route Response (RREP)

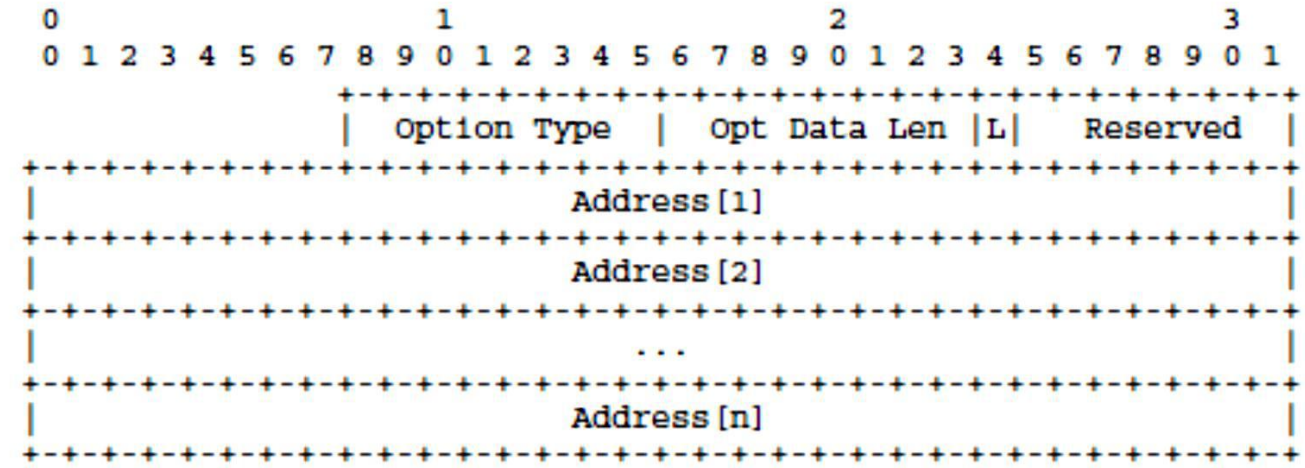

Figura 2.14 Formatul mesajelor Route Response (RREP). [28]

Formatul mesajelor Route Response (RREP) este alcatuit din:

- Tipul opţiunii: valoarea câmpului este setat cu 2, pentru pachete de tip Route Reply.
- Opt Data Len: lungimea pachetului RREP.

- L (Last Hop External): fanion care indică ultima adresă din pachetul RREP care corespunde unui nod de legătură cu o reţea wireless externă.
- Rezervat: ignorat la recepţie. este setat cu valoarea 0.
- Adresa [n]: adresele care fac parte din ruta inversă .

Formatul mesajelor Route Error (RERR)

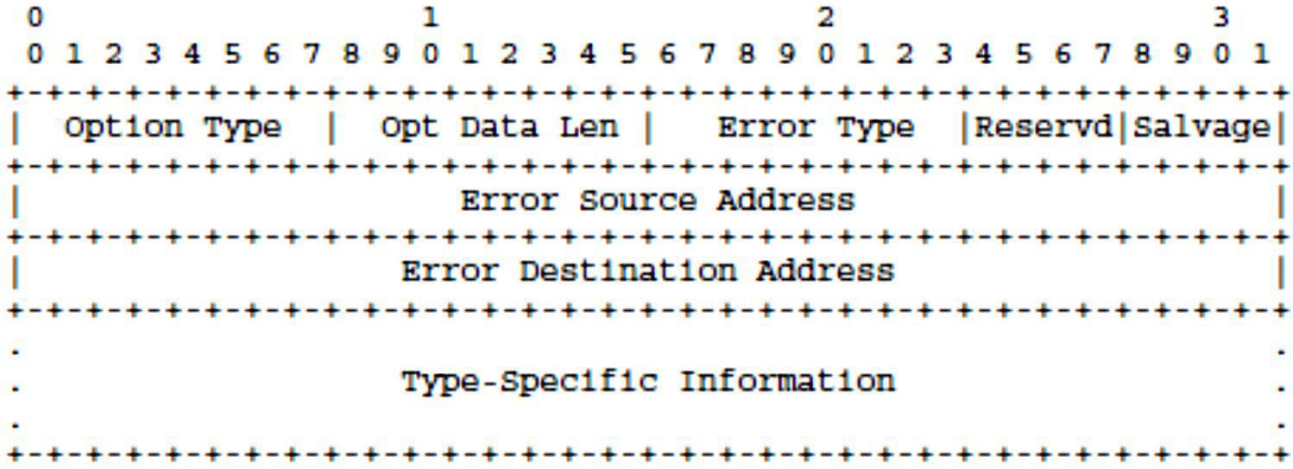

Figura 2.15 Formatul mesajelor Route Error (RERR). [28]

Formatul mesajelor Route Error (RERR) este alcatuit din :

- Tipul opţiunii: valoarea câmpului setat cu 3, pentru pachete de tip Route Error.
- Opt Data Len: lungimea opţiunii RERR în octeţi.
- Tipul erorii: tipul erorii întânite.
- Rezervat: ignorat la recepţie.
- Adresa sursă eroare: adresa nodului care a generat pachetul RERR.
- Adresa destinaţie eroare: adresa nodului căruia pachetul RERR este destinat.
- Informaţie specifică tipului erorii: informaţii suplimentare legate de tipul erorii.

Probleme de performanţă

O parte dintre caracteristicile protocolului DSR afectează performanţele acetuia şi îl fac vurnerabil la unele atacuri [1 de la diana] :

Ne-expirarea rutelor: protocolul DSR nu detine un mecanism eficient de a înlătura rutele învechite , cache-ul nodurilor mobile va fi ocupat cu tabele de rutare ce pot conţine căi întrerupte. Folosirea acestor rutelor învechite poate duce la pierderi de pachete şi consuma din lărgimea de bandă a reţelei. Din cauza că nodurile intermdiare îşi crează în cache rute proprii nu ajută prea mult performanţa rutării. În momentul în care aceste rute se învechesc, iar nodurile răspund la o cere de rută, având calea către detinaţie salvată în cache, tabelele de rutare ale nodurilor intermediare până la sursă şi inclusiv destinatie vor fi poluate cu informaţii învechite.

Salvarea datelor. Dacă un nod intermediar întâlneşte o legătură întreruptă şi are o cale alternativă către destinaţie, acesta va încerca să salveze datele prin transmiterea lor pe calea alternativă. Acest lucru este util în cazul unor reţele statice, dar în cazul reţelelor extrem de dinamice cu sunt

reţelele ad hoc este foarte posibil ca ruta alternativă sa fi fost învechită. Prin urmare astfel de acţiuni pot dăuna mai mult decât pot ajuta.

Scurtarea automată a rutelor. Atunci când un nod, recepţionează pachete ce nu îi sunt destinate, verifică dacă nu cumva, acestea pot fi rutate prin intermediul său pentru a scurta ruta. Dacă acest lucur este posibil, va trmite sursei un mesaj pentru a o informa de ruta mai scurtă. La fel ca şi în cazul precedent o astfel de acţiune pe lâncă evidentele beneficii, poate afecta performanţa şi chiar securitea reţelelor.

2.7 Înbunatatiri şi optimizări

Securitatea

Ca şi în cazul celorlalte protocoale de rutare , securitatea pentru AODV are o importanţă foarte mare. Securitarea este necesară rutării în faţa unor inamici care au acces la mediul de comunicaţii. Autentificarea şi metodele de păstrare a confidenţialităţii care au fost adoptate pentru alte protocoale de rutare sunt considerate a fi suficiente pentru AODV, deoarece acest protocol prezintă puţine vulnerabilităţi în ceea ce priveşte atacurile ce pot afecta rutarea.

Rutarea asimetrică

Există multe cazuri în care presupunerea simetriei legăturilor dintre noduri vecine să nu fie validă. În astfel de reţele AODV prezintă un avantaj şi anume o extensie a pachetului Hello care include lista vecinilor cunoscuţi ai nodului respectiv. Dacă un nod primeşte un astfel de mesaj Hello, dar care nu conţine adresa să IP, atunci acesta realizează că legătura cu acest nod este unidirecţională şi nu trebuie să trimită nici un pachet nodului respectiv.

Rutarea asimetrică pune probleme serioase la translatarea unei adrese IP într-o adresă MAC (deci de nivel 2). Deoarece ARP (Address Resolution Protocol), protocolul care stabileşte corespondenţele între adresele IP şi adresele MAC, presupune existenţa unei conectivităţi bidirecţionale, prin urmareca şi în cazul rutării asimetrice rezoluţia de adrese trebuie stabilită după algoritmi speciali. Totuşi, stabilirea rutelor asimetrice este importantă, iar AODV se doreşte a fi configurat pentru a oferi această funcţionalitate.

Pentru a favoriza legăturile simetrice prin dezactivarea celor asimetrice, este necesară o strategie de înştiinţare. Fiecare nod care recepţionează un pachet RREP trimite apoi un pachet RREP-ACK (o confirmare a primirii pachetului) înapoi către nodul care a trimis pachetul iniţial. Dacă un nod primeşte pachetul RREP, atunci ştie că legătura este bidirecţionala deoarece pachetul RREP răspunsul la cererea de rută. Iar pachetul de confirmare, RREP-ACK garantează bidirecţionalitatea către următorul nod. [29]

Capitolul 3. Analiză experimentală şi implementare

În acest capitol este descris modul în care se desfăşoară studiul de performanţă a celor mai reprezentative protocoale de rutare utilizate în rețelele de ad-hoc. Mai precis, se ocupă cu aspectele metodologice, cum ar fi procedura de evaluare, metode de evaluare, scenarii şi parametri, limitări implicite şi domeniul de aplicare al studiului, dar şi cu analiza şi interpretarea rezultatelor bazate pe acest studiu.

3.1 Platforma de evaluare

Mediul de simulare utilizat in acest proiect este OPNET. Acesta este o unealta foarte sofisticată și oferă o interfață grafică foarte atractivă pentru utilizator. Este utilizat în special pentru simulările de rețea ce includ cercetarea și dezvoltarea rețelelor. OPNET se numără printre cele mai importante simulatoare care sunt utilizate în clipa de față. Marea majoritate a celelorlalte simulatoare nu au la dispoziție o librarie la fel de vastă precum OPNET-ul o are. Cu acest program se poate atinge o înțelegere mai avansată a protocoalelor de rutare, dispozitivelor de rețea și a scenariilor de rețea și toate acestea într-un mod foarte eficient.

Cu ajutorul acestui software se pot simula o gamă largă de reţele cu fir şi wireless; este dea asemenea prezentă şi implementarea nivelului MAC IEEE 802.11. Deşi principalul scop este diagnosticarea şi reorganizarea reţelelor companiilor, este posibilă şi implementarea unor algoritmi noi folosind resursele deja existente. În general modelarea este făcută pe baza unei interfeţe grafice ierarhice; se pot simula reţele cu un număr de câteva sute de noduri.

OPNET Modeler include un instrument de analiză şi librării ale modelelor, realizând modelarea pe baza unei structuri ierarhice. La nivelul de jos, care este şi cel personalizabil, modelele de procese sunt structurate ca maşini cu stări finite. Stările şi tranziţiile pot fi specificate folosind diagrame de stare, pe când condiţiile care determină fiecare stare sunt implementate într-un limbaj asemănător cu „C” numit „Proto-C”. Modelele de proces şi modulele înglobate în OPNET (modulele sursă şi destinaţie, generatoarele de trafic, modulul wireless) sunt apoi configurate cu meniuri şi organizate în diagrame de flux de date care reprezintă nodurile, prin folosirea unui editor de noduri. Nodurile şi linkurile care construiesc topologia reţelei sunt selectate prin utilizarea unui editor de reţea. Vizualizarea şi manipularea datelor colectate în timpul simulării este făcută de către un instrument de analiză; rezultatele obţinute pot fi vizualizate pentru orice element al reţelei în parte sau global.

Librăriile cu modele conţin protocoale şi tehnologii de telecomunicaţii (de exemplu, TCP/IP, Frame Relay, Ethernet, IEEE 802.11), tipuri de legături (punct-la-punct sau magistrală).

În privinţa tehnologiilor wireless, sunt prezente module pentru reţele locale, GSM şi ad-hoc. OPNET include protocolul MAC 802.11 şi protocoalele de rutare AODV, DSR şi TORA.

3.2 Indicatorii de performanta

3.2.1 Throughput

Throughput-ul se referă la rata medie de transfer a datelor care ajung cu succes la destinație trecând printr-un numar de noduri intermediare pe un canal de comunicații. Rata medie de transfer din

rețea este măsurată în biți pe secundă (bps). Un throughput de valoare mare reprezintă adesea o necesitate în cazul tuturor tipurilor de rețele.
Formula matematică a thrughput-ului este:

$$T = \frac{numarul\ \ de\ biti}{timpul\ \ de\ observatie}.$$

3.2.2 Întârzierea capăt la capăt

Întârzierea capăt la capăt se referă la timpul necesar pachetelor de date să traverseze reţeaua de la o sursă care o destinaţie.
Acest parametru evaluează performantele protocoalelor de rutare în termeni de folosire eficientă a resurselor reţelei. Acest indicator ia in calcul numai pachetele care ajung cu succes la destinatie.

Formula matematică pentru întârzierea capăt la capăt este:

$$\tau=\frac{\sum(\tau\ \text{receptie}\ -\tau\ \text{transmisie}\ )}{\sum \text{N conexiuni}}.$$

3.2.3 Procentul de recepţie a pachetelor

Procentul de recepţie a pachetelor se se referă la numărul procentului de pachete transmise de către 0 sursă care ajung la o destinaţie. Aceast indicator de performanţă oferă o idee asupra modului în care protocolul excelează în termeni de transmisia de pachete la viteze diferite şi pentru modele diferite de trafic.

Formula matematică pentru procentul de recepţie a pachetelor este:

$$P=\frac{\sum \text{Nr pachete receptionate}}{\sum \text{Nr pachete trimise}}.$$

3.2.4 Încărcătura de rutare normalizată

Încărcătura de rutare normalizată se referă la numărul de pachete de control (pachete de rutare) trimise de către toate nodurile din reţea supra numărul de pachete de date recepţionate la destinaţie.

Formula matematică pentru încărcătura de rutare normalizată este:

$$I= \frac{\sum \text{Nr pachete de rutare}}{\sum \text{Nr pachete de date}}$$

3.3 Modelarea reţelei ad hoc

Cele mai importante componete folosite în construirea unei reţele ad hoc sunt prezentate în acest subcapitol.

Plecand de la nivelul 7 al stivei OSI în jos, cea mai importantă componentă analizată va fi cea de aplicaţie. Având în vedere faptul că în realitate ceea ce ne interesează este să avem posibilitatea de a folosi aplicaţii uşor şi rapid , configuraţia aplicaţiei are un rol important în conceperea unei reţele. Unele dintre cele mai uzuale aplicaţii de reţea care sunt destinate folosirii în Internet sunt: pagini web, mail, servere etc. În spatele acestor aplicaţii există un protocol al nivelului aplicaţie. De exemplu pentru

pagini web este folosit protocolul HTTP, pentru schimb de fişiere este folosit protcolul FTP etc. Traficul de date folosit în simulările care vor urma este de tip FTP. Nivelul transport (nivel 5 OSI) este responsabil cu generarea şi recepţionarea pachetelor.

La nivel reţea vom folosi pe rând protocoalele DSR, AODV, TORA, aceste protocoale sunt utilizate pentru a dirija pachetele de date de la sursă către destinaţie în reţele ad-hoc.

Nivelul legătură (LL-Link Layer) se ocupă cu fragmentarea şi reasamblrea pachetelor, la ceste nivel rulează protocolul ARP, folosit pentru a crea corespundeţe între adresele IP ale nodurilor şi adresele MAC ale acestora. [30]

Nivelul Mac foloseşte drept protocol IEEE 802.11 care a fost descris in capitolul care utilizeaza mesaje de tip RTS/CTS/DATA/ACK. [30]

Interfeţele de reţea constu în ineterfeţe hardware folosite de nodurile mobile pentru a accesa canalul. Prin acestea se simulează integritatea semnalului, coliziunile.

Modelul de propagare radio foloseşte atenuarea de tip Two ray ground pentru distanţe mari. Decide dacă pachetele pot fi sau nu recepţionate de nodul mbil, dată fiind o anumită destanţă , o anumită putere de transmisie şi o anumită lungime de undă. [30]

Modelul de reflexie Two ray ground ia în considerare atât calea directă cât şi calea reflectată. Puterea de recepţie pentru o distanţă " d" este dată de formula:

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L}$$

Unde :

P_t = puterea de transmise a semnalului

G_t , G_r = câştigurile antenelor dispozitivelor emiţător respectiv receptor

h_t, h_r = înălţimile antenelor dispozitivelor emiţător respectiv receptor

L = piederea de sistem

3.4 Scenarii

Alegerea scenariilor reprezintă cea mai importantă acţiune într-un studiu simulativ. Arhitectura reţelei, modul în care nodurile interacţionează, şi în acest caz modul în care acestea se deplasează sunt factori cheie care decid rezultatele simulărilor. Unele scenarii pot pune în evidenţă un anumit protocol, care se adaptează cel mai bine condiţiilor respective din reţea. Acesta poate să nu fie însă cel mai eficient, sau poate avea, pentru un alt scenariu, rezultate foarte proaste. Am vazut în capitolele teoretice că anumite protocoale funcţionează bine pentru anumite reţele şi nu aşa bine pentru arhitecturi mai complexe de exemplu. Prin urmare, un singur scenariu nu poate oferi rezultate finale cu privire la performanţa unui astfel de protocol de rutare. Ca atare, este nevoie de simularea mai multor arhitecturi de reţea pentru diferiţi parametri ai acesteia. Având în vedere faptul că protocoalele de rutare nu sunt de sine stătătoare şi depind foarte mult şi de alte protocoale precum cele de la nivelul Legătura de Date sau cele de la nivelul Transport, în alcătuirea scenariilor trebuie să se ţină cont şi de aceste elemente.

Să nu uităm nici de factorul mobilitate, care este esenţial în reţelele ad hoc. Mobilitatea este parametrul cheie pentru a simula o reţea cât mai apropiată de realitate. Totodată, mai avem şi factorul congestie care impune câteva probleme protocoalelor. Pe lângă acestea mai intră în calcul şi dimensiunea reţelei, reprezentată de numărul de noduri care o alcătuiesc.

3.4.1 Scenariul Eveniment

Scopul acestei topologii este de a pune în evidenţă funcţionarea protocoalelor de rutare AODV ,DSR, TORA în cazul unei mobilităţi medii (aproximativ 1.5 metri pe secundă) şi un număr de 15 , 30 şi 60 de noduri mobile.

În cazul scenariului Eveniment am propus o arhitectura de reţea ce ar replica modul de comportare a indivizilor aflaţi la un anumit eveniment, fie acesta un eveniment politic. Ideea de bază este aceea că în cadrul evenimentului desfăşurat indivizii, posesori a unor dispozitive mobile vor comunica cu un server (de asemenea mobil), folosind reţele ad hoc. Îi putem considera pe aceştia reporteri care îşi transmit datele serverului spre a fi stocate şi prelucrate în prealabil sau care accesează pagini web pentru a le folosi în cadrul reportajului. Aceştia sunt amplasaţi în puncte marginale ale reţelei şi se vor folosi de dispozitivele mobile ale altor indivizi care nu comunică pentru a ruta trafic către serverul aflat undeva în centrul reţelei. Totodată, toate dispozitivele mobile prezente vor dispune de o mobilitate caracterizată de o viteză de 1.5 m/s (viteză tipică mersului pe jos la oameni) şi o traiectorie aleatoare (bazata pe modelul de mobilitate Random Waypoint Mobility).

Problema care se pune, în cadrul acestui scenariu este evaluarea performanţelor celor trei protocoale de rurtare specifice reţelelor ad hoc (AODV, DSR, TORA) din punct de vedere al impactului creşterii dimensiunii reţelei. În cadrul acestei topologii viteza mobilelor este una scazută, deoarece nu se doreşte ca factorul mobilitate să aibă o influenţă decisivă asupra măsurătorilor.

Dimensiunea reţelei a fost variată utilizând câte 15, 30 şi respectiv 60 de noduri mobile. Din punct de vedere al modelării dispozitevelor mobile am considerat că o rază maximă de transimisiune de aproximativ 275 m va fi suficientă pentru a pune în vedere mecanismul de rutare.

În cele ce urmează vor fi prezentate cele trei topologii pentru scenariul Eveniment.

3.4.1.1 Detalii de implementare

Parametri de configurare a reţelei :

- Parametri generali

Parametri	
Numărul de noduri mobile	15
Protocolul de rutare	AODV,DSR,TORA
Dimensiunea reţelei (X)	1000 m
Dimensiunea reţelei (Y)	1000 m
Durata simulării	3 min
Tipul de trafic	TCP
Tipul de aplicaţie	FTP,HTTP
Viteza nodurilor	1.5m/s

Tabel 3.1 Parametri generali

- Parametrii WLAN

Data Rate	11Mbps
Puterea de Transmisie	0.0003
Puterea de recepţie a datelor-prag	-95
Opţiunea CTS-to-self	Enabled
Limita Short Retry	7

Limita Long Retry	4
Intervalul AP Beacon	0.02
Max Receive Lifetime	0.5
Dimensiune Buffer	256000

Tabel 3.2 Parametrii WLAN

- Parametri FTP

Parametrii	
Command Mix	100%
Inter-Request Time	Constant(5)
File Size	Constant(50000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort(0)
Operation Mode	Serial (Ordered)
Start Time	Constant(0)
Duration	End of Simulation
Inter-repetition Time	Constant(1)
Number of Repetitions	Unlimited
Repetition Pattern	Serial

Tabel 3.3 Parametri FTP

- Parametrii de mobilitate

Parametrii	
Modelul de mobilitate	Random Waypoint Mobility
x_min	0.0
y_min	0.0
x_max	500
Viteza	Constant(1.5)
Pause Time	Uniform(0.2)
Start Time	Consant(0)
Stop Time	End of Simulation

Tabel 3.4 Parametrii de mobilitate

3.4.1.2 Rezultate

Parametri de performanţă	DSR	AODV	TORA
Throughput [kbps]	544.65	465.26	297.56
Întârzierea capăt la capăt [ms]	14.55	3.096	7.172
Traficul de rutare recepţionat	6179.436	54689.36	54154.06
Nr. de pachete pierdute	6538.612	6727.978	16757.23

Tabelul 3.5 Parametrii de performanţă pentru scenariul eveniment 15 noduri.

Parametri dperformanţă	DSR	AODV	TORA
Throughput [kbps]	769.65	670.45	371.95
Întârzierea capăt la capăt [ms]	9.595	2.342	6.917
Traficul de rutare recepţionat	10409.78	139592.1	166755.6
Nr. de pachete pierdute	10367.407	3789.054	4863.746

Tabelul 3.6 Parametrii de performanţă pentru scenariul eveniment 30 noduri.

Parametri dperformanţă	DSR	AODV	TORA
Throughput [kbps]	936.28	1088.96	325.09
Întârzierea capăt la capăt [ms]	8.66	2.374	11.875
Traficul de rutare recepţionat	19822.06	313032.3	699326.3
Nr. de pachete pierdute	15382.76	13337.5	12159.8

Tabelul 3.7 Parametrii de performanţă pentru scenariul eveniment 60 noduri.

3.4.1.3 Scenariul Eveniment 15 noduri

Topologia reţelei cuprinde 15 noduri mobile, dintre care 4 noduri transmit trafic FTP iar un nod recepţionează. Arhiectura acestui scenariu este prezentată în figura de mai jos:

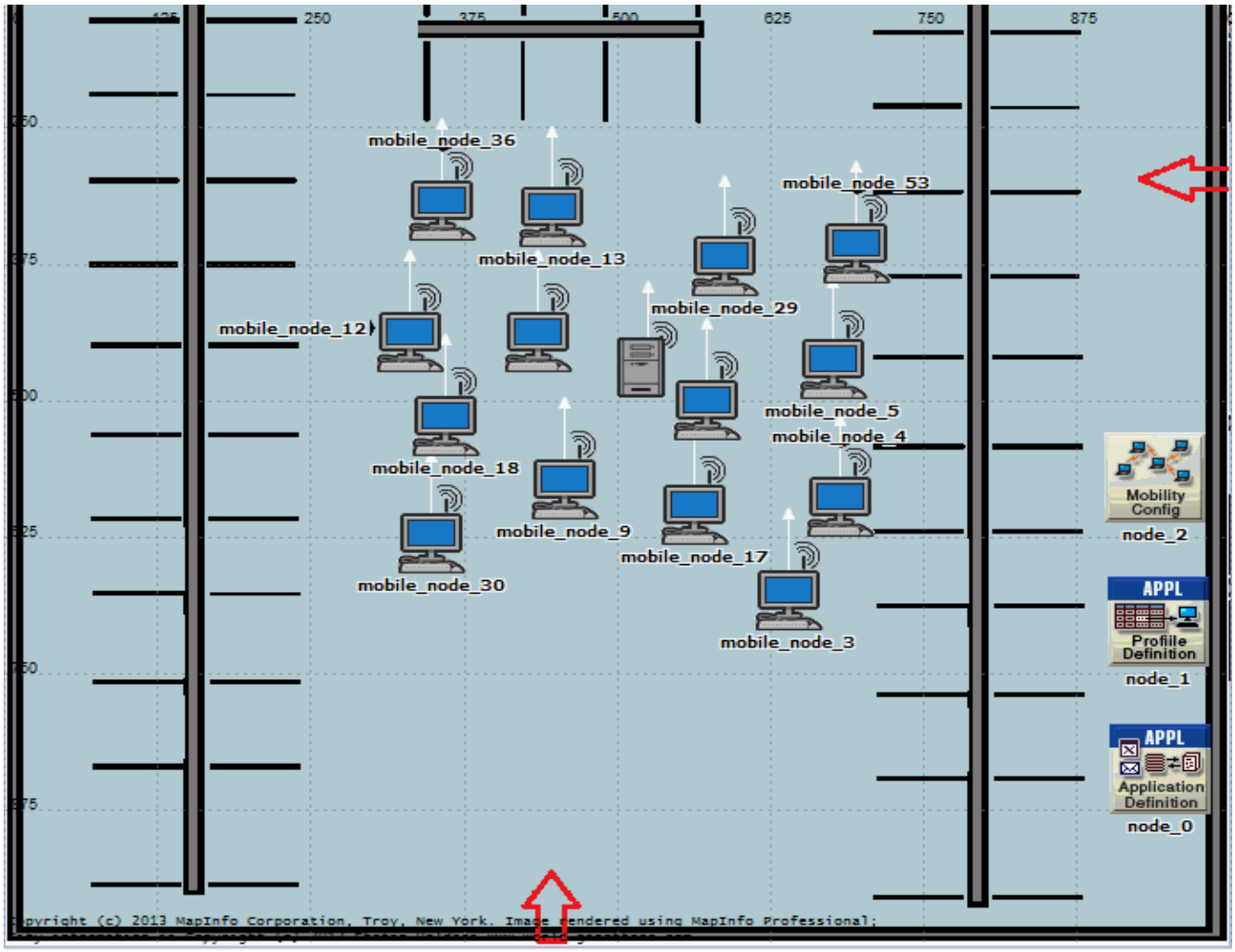

Figura 3.1 Arhitectura de reţea pentru scenariul Eveniment cu 15 noduri mobile

Rezultatele simulării

Rezultatele simulării vor fi prezentate sub formă grafică şi vor ilustra o serie de indicatori de performanţă importanţi pentru analiza în cauză. Aceşti indicatori vor fi Throghput ,Delay, Data Loss şi Traficul de rutare recepţionat. Rezultatele vor fi prezentate în paralel în cadrul aceluiaş grafic atât pentru protocolul de rutare AODV cât şi pentru DSR şi TORA.

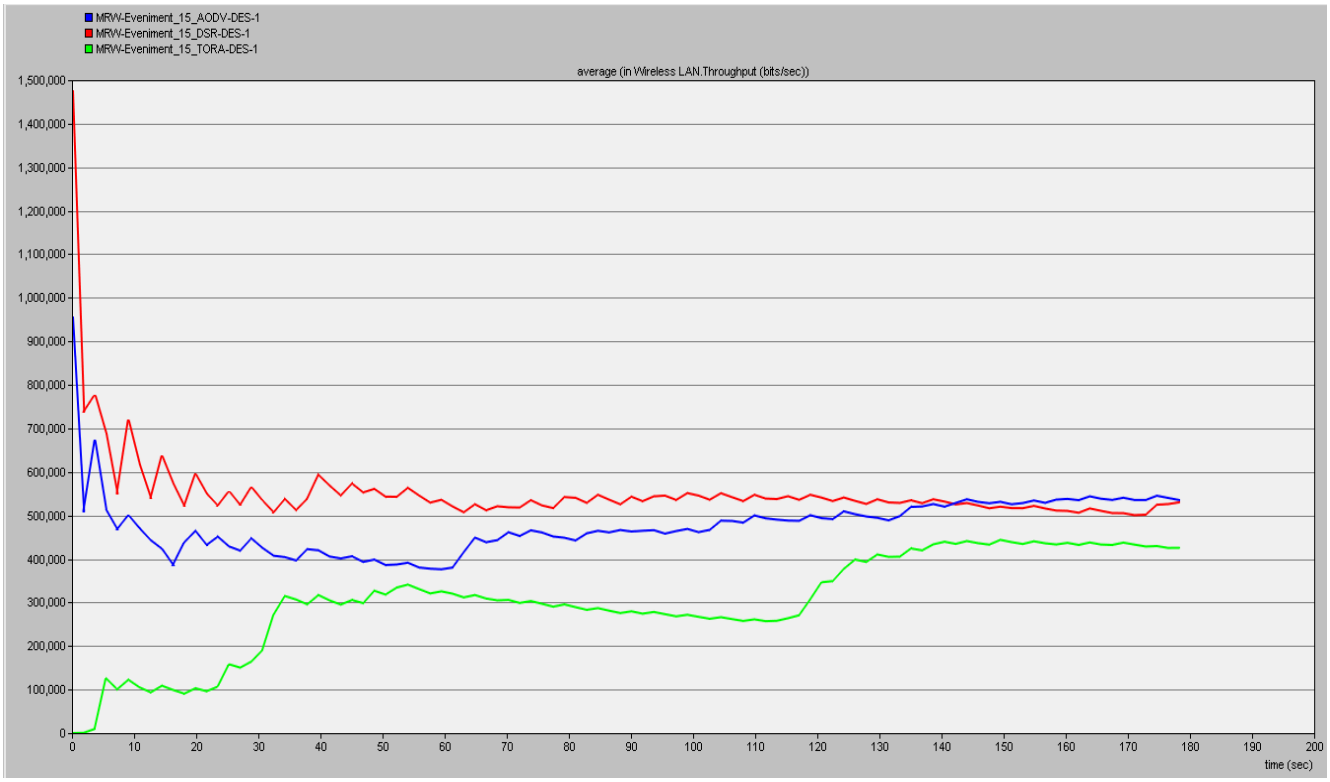

Figura 3.2 Analiza protocoalelor AODV şi DSR din punct de vedere al indicatorului de performanţă Throughput.

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra throughput-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra throughput-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra throughput-ul protocolului TORA.

Analiza rezultatelor:

Din grafic observăm că valoarea throughput-ului în cazul protocolului DSR este în primcipiu mai mare faţă de cea a protocolului AODV. Diferenţa dintre acestea nu este însă chiar aşa de mare. Valorile mari ale throughputului la începutul simulării apar datorită iniţierii schimbului de mesaje de rutare în întreaga reţea lucru ce duce la o astfel de încărcare. Pe parcursul simulării perfomranţele DSR în ceea ce priveşte throughput-ul se dovedesc a fi uşor mai crescute faţă de AODV.
Throughputul protocolului TORA prezintă cele mai jose valori. Interesant este ca, spre deosebire de protocoalele precedente valoarea de inceput a acestui parametru este foarte mica. Acest lucru are drept cauză maniera diferită în care TORA îşi construieşte căile. Reţeaua nu mai este invadată cu mesaje de control, acestea implicând în general un numar mic de noduri.
Spre finalul simulării se observă o stabilitate în valoarea traficului şi totodată o uşoară creştere a acestuia. Acest lucru se datorează faptului că nodurile devin din ce în ce mai apropiate iar rata de transmisie a datelor creşte odată cu aproprierea acestora.

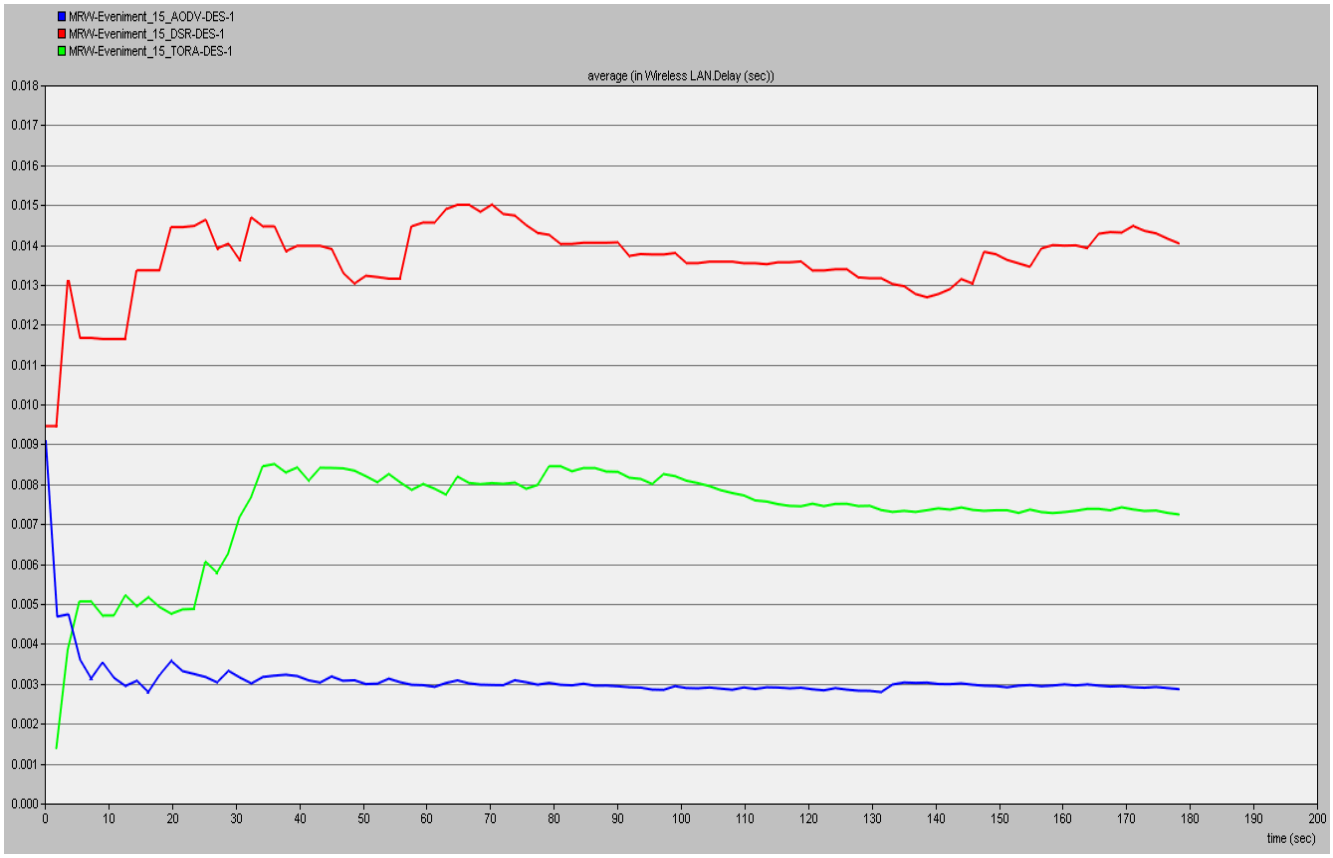

Figura 3.3 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Delay

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra delay-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra delay-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra delay-ul protocolului TORA.

Analiza rezultatelor:

Graficul ne arată că delayul care apare în cazul protocolului DSR este cu mult mai mare faţă de cel corespunzător protocolului AODV sau protocolului TORA. Acest fenomen apare datorită faptului că protocolul DSR foloseşte rute cu un număr mai mare de hopuri faţă de cele folosite de AODV. Un număr mai mare de hopuri presupune un timp mai mare de procesare şi deci o valoare a întârzierii mai mare. Sigur întârzierea este de ordinul milisecundelor iar o diferenţă de 10 milisecunde nu ar fi remarcată de utilizatorii de date. Problema apare în cazul în care reţeaua ar fi mai mare iar numărul de hopuri până la destinaţie ar creşte. Probabil ca într-o astfel de reţea performanţa protocolului DSR în ceea ce priveşte acest parametru nu ar mai fi aşa bună. AODV are o întârziere foarte mică lucru explicat prin mecanismul mult mai bun de găsire a rutelor. TORA este undeva la mijloc, din acest punct de vedere. Optimizarea drumurilor are o importanta secundară în contextul acestui protocol, căile lungi pot fi utilizate în scopul evitării declansării unui nou proces de descoperire de noi rute. În comparaţie cu DSR însă, la TORA nu există posibilitatea de a învăţa rute învechite.
Aşadar în acest caz protocolul AODV se dovedeşte a fi mai performant decât DSR şi TORA.

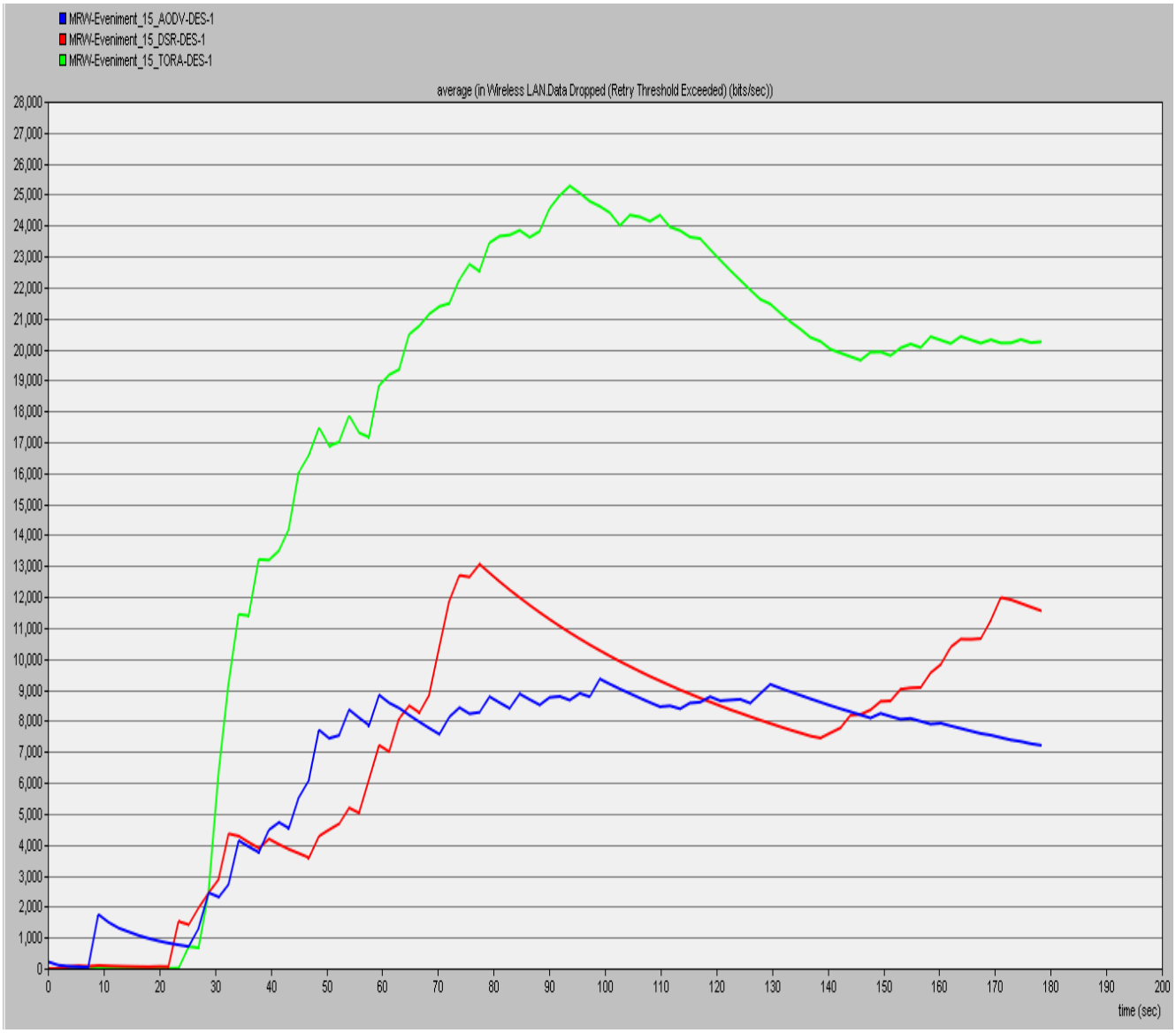

Figura 3.4 Analiza protocoalelor AODV, DSR, TORA din punct de vedere al indicatorului de performanţă Data Loss

Observaţie: La fel ca şi în cazurile precedente culoarea albastra corespunde protocolului AODV culoarea roşie protocolului DSR iar cea verde este asociată protocolului TORA.

Analiza rezultatelor:

Din punctul de vedere al pachetelor pierdute protocoalele AODV şi DSR prezintă performanţe asemănătoare, pierderile sunt datorate în mare parte mobilităţii nodurilor. Putem observa că la un moment dat DSR prezintă valori ceva mai mari faţă de AODV. Acest moment corespunde celui în care ruta folosită iniţial de către DSR este pierdută şi acesta trebuie să descopere o nouă rută către destinaţie. TORA atinge valori ale pierderilor aproape duble faţă de celelalte două protocole studiate. Prin urmare este cel mai slab protocol din acest punct de vedere.

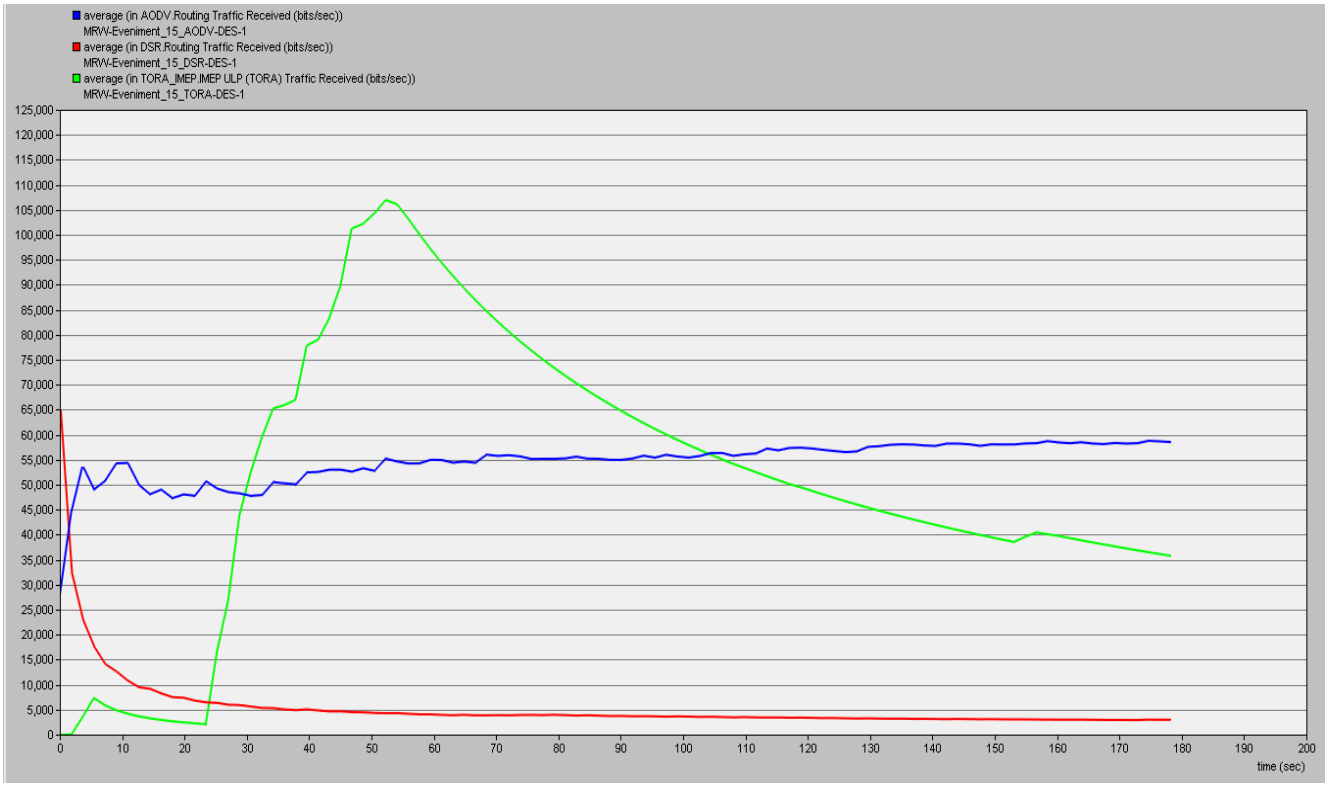

Figura 3.5 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al traficului de rutare recepţionat

Analiza rezultatelor:

Traficul de rutare în cazul AODV este cu mult mai mare decât traficul de rutare corespunzător DSR. Acest trafic apare datorită mişcării continue a nodurilor. Mobilitatea cauzează schimbări în topologia reţelei iar acestea schimbări cauzează declanşări ale mecanismului de descoperire de rute care inundă reţeaua cu trafic de rutare. Acest lucru se întâmplă foarte des în cazul protocolului AODV datorită timpilor de expirare şi mecanismului de împrospătare de rute şi rar în cazul protocolului DSR care nu pierde aşa uşor rutele având de altfel un mecanism prin care poate descoperi rute alternative fără a mai fi necesar un nou proces de descoperire de rute. În cazul protocolului TORA se observă că traficul cauzate de mesajele de control are valori scăzute la începutul simulării, datorită faptului că TORA implică în procesul descoperirii rutelor un număr mic de noduri. Totodată, acesta începe să crească la valori mult mai ridicate faţă de cele ale celorlalte protocoale. Acest lucru denontă faptul că a fost iniţiat un nou proces de descoperire a rutelor (creare a graficului). Se observă că momentul creşterii numărului de pachete de rutare corespunde momentului creşterii numărului de pachete pierdute. Acest lucru se explică prin faptul că TORA are nevoie de mai multe retransmisii a pachetelor de control înainte de a putea transmite date.

3.4.1.4 Scenariul Eveniment 30 noduri

Topologia rețelei cuprinde 30 noduri mobile, dintre care 4 noduri transmit trafic FTP iar un nod recepționează. Arhiectura acestui scenariu este prezentată în figura de mai jos:

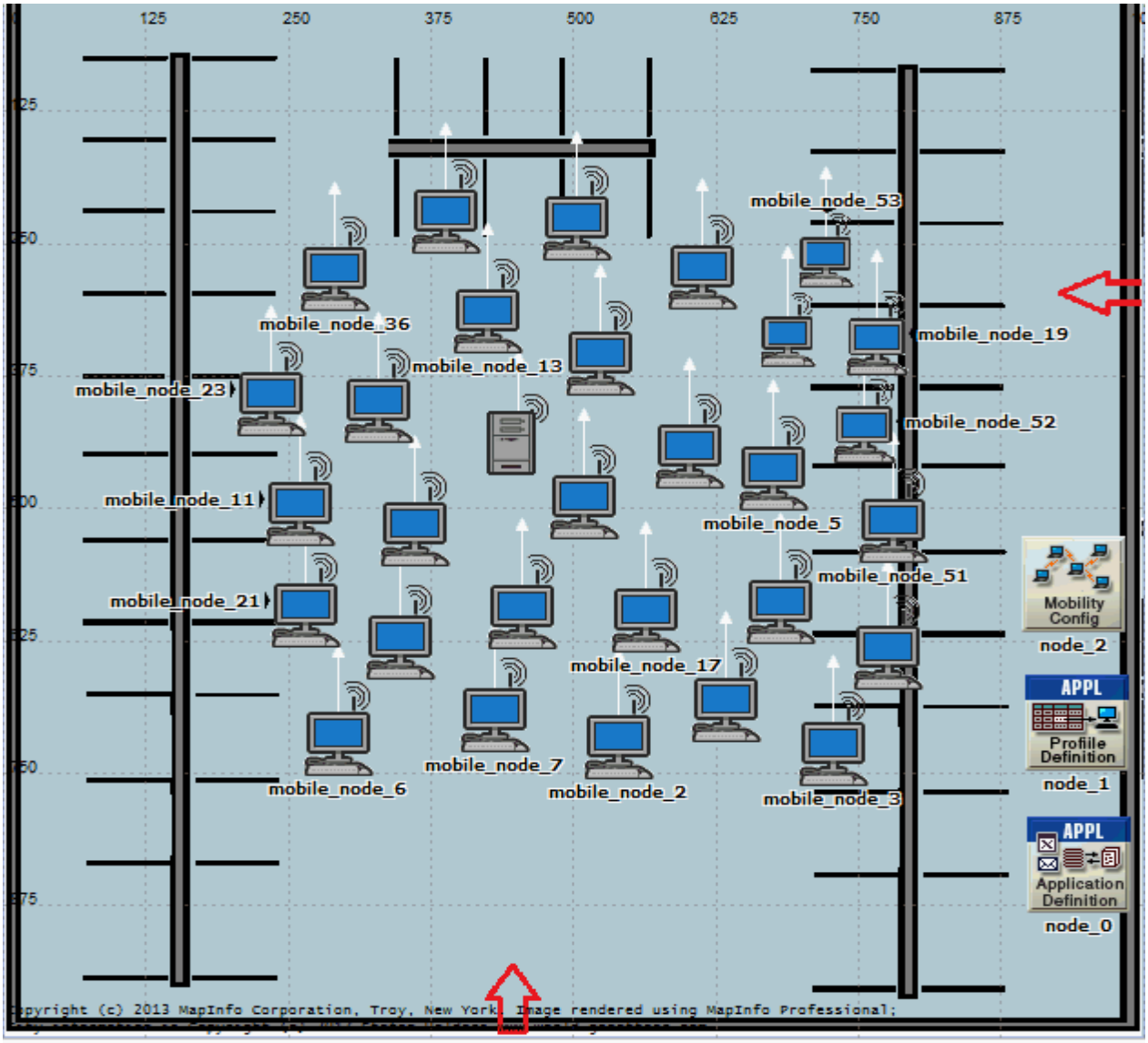

Figura 3.6 Arhitectura de rețea pentru scenariul Eveniment cu 30 noduri mobile

Rezultatele simulării:

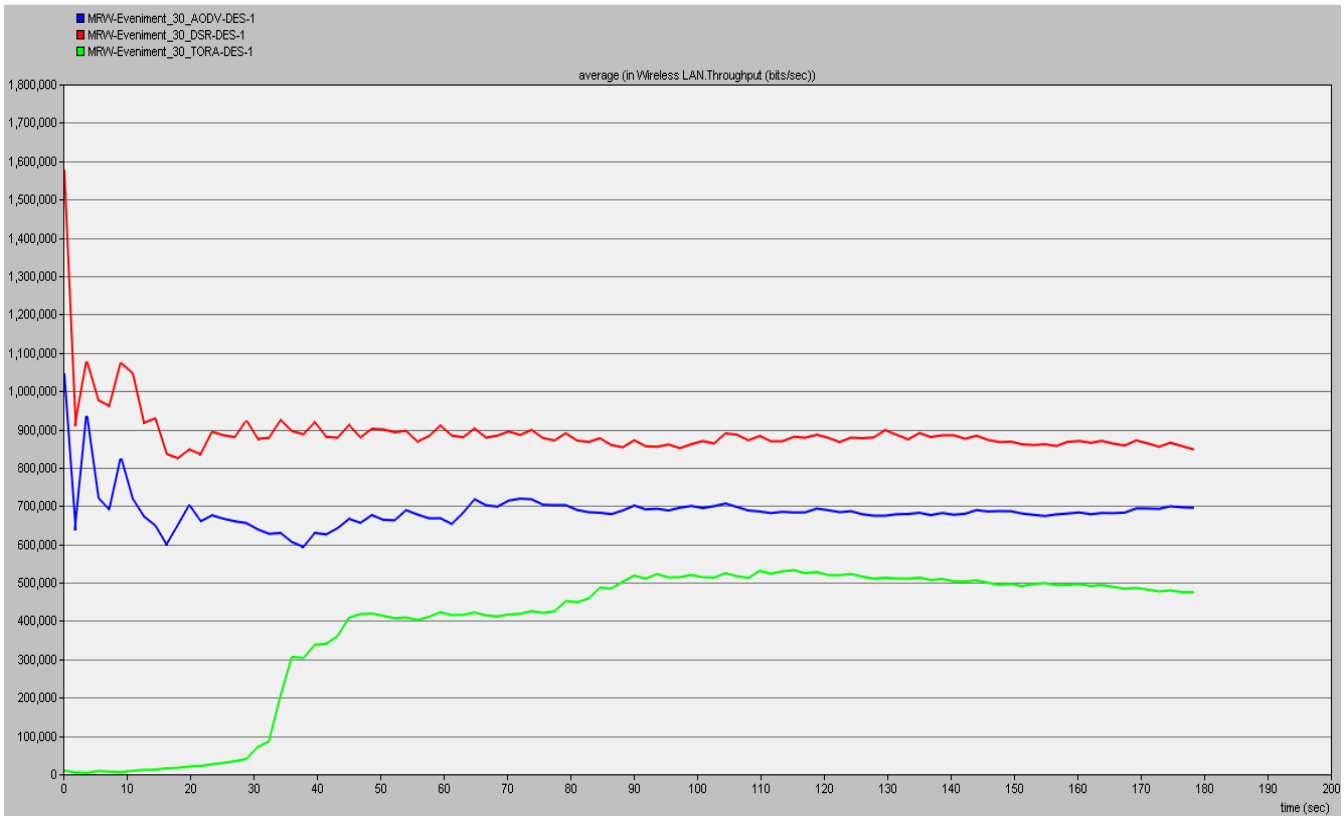

Figura 3.7 Analiza protocoalelor AODV, DSR , TORA din punct de vedere al indicatorului de performanţă Throughput

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra throughput-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra throughput-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra throughput-ul protocolului TORA.

Analiza rezultatelor:

Din grafic observăm că valoarea throughput-ului în cazul protocolului DSR este şi în acest caz este ceva mai mare decât cea a protocoalelor AODV, respectiv TORA. Comportamentul celor două protocoale AODV şi DSR este similar. La începutul simulării avem un throughput mare datorită iniţierii schimbului de mesaje de rutare în întreaga reţea iar pe parcurs aceasta se stabilizează la o valoare datorită aproprierii de nodul destinaţie. Ca şi în cazul scenariului cu 15 noduri TORA prezintă performanţe la fel de scăzute faţă de celelalte două protocoale studiate.

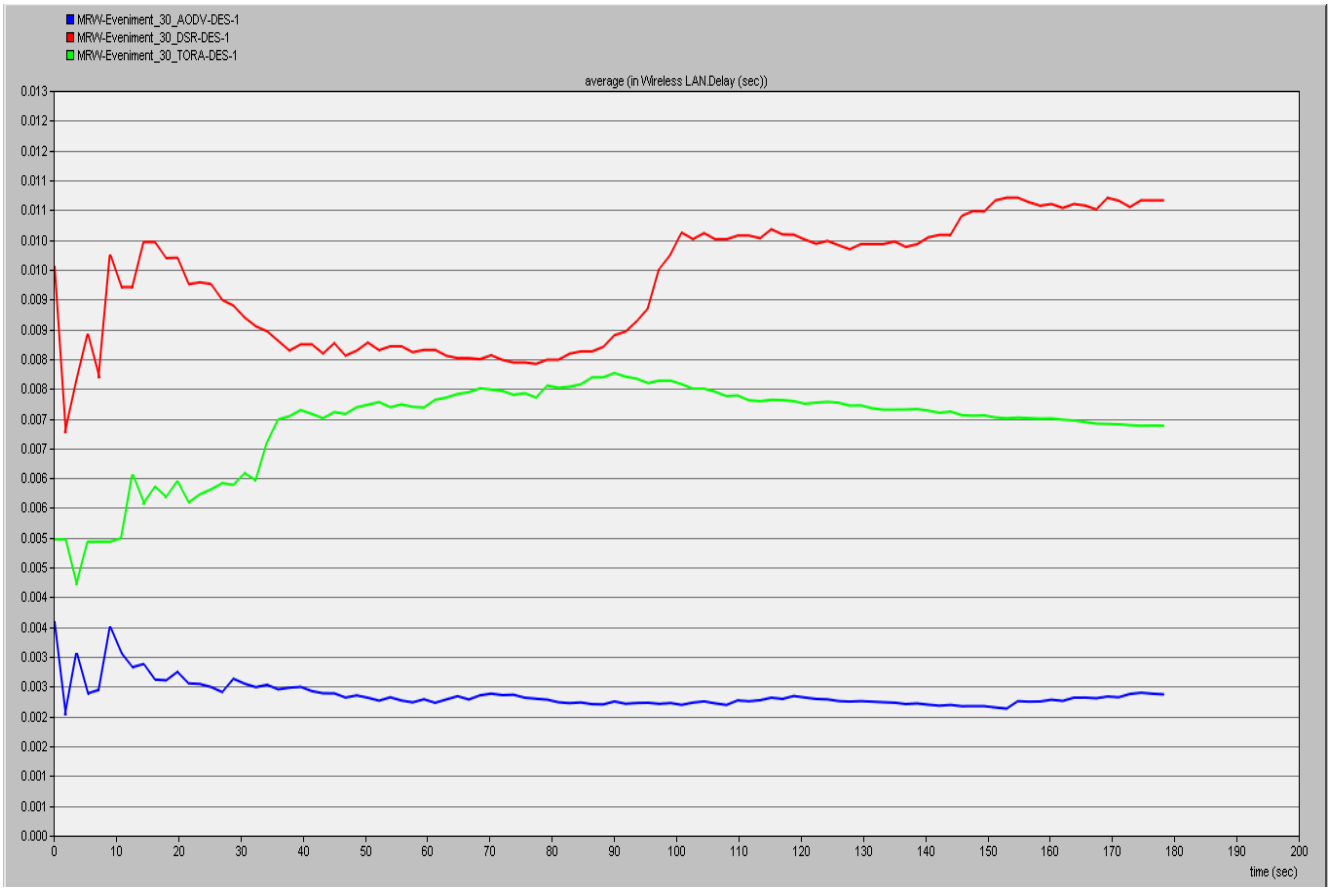

Figura 3.8 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Delay

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra delay-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra delay-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra delay-ul protocolului TORA.

Analiza rezultatelor:

Din punct de vedere al delayului protocolul DSR prezintă din nou perfomanţe mai scăzute faţă de AODV şi TORA. Această diferenţă rămâne însă mică deşi am dublat dimensiunea reţelei. Observăm însă că dublarea dimensiunii reţelei are un impact negativ asupra delay-ului în cazul protocolului TORA. Acesta prezentând valori ceva mai ridicate faţă de cazul precedent.

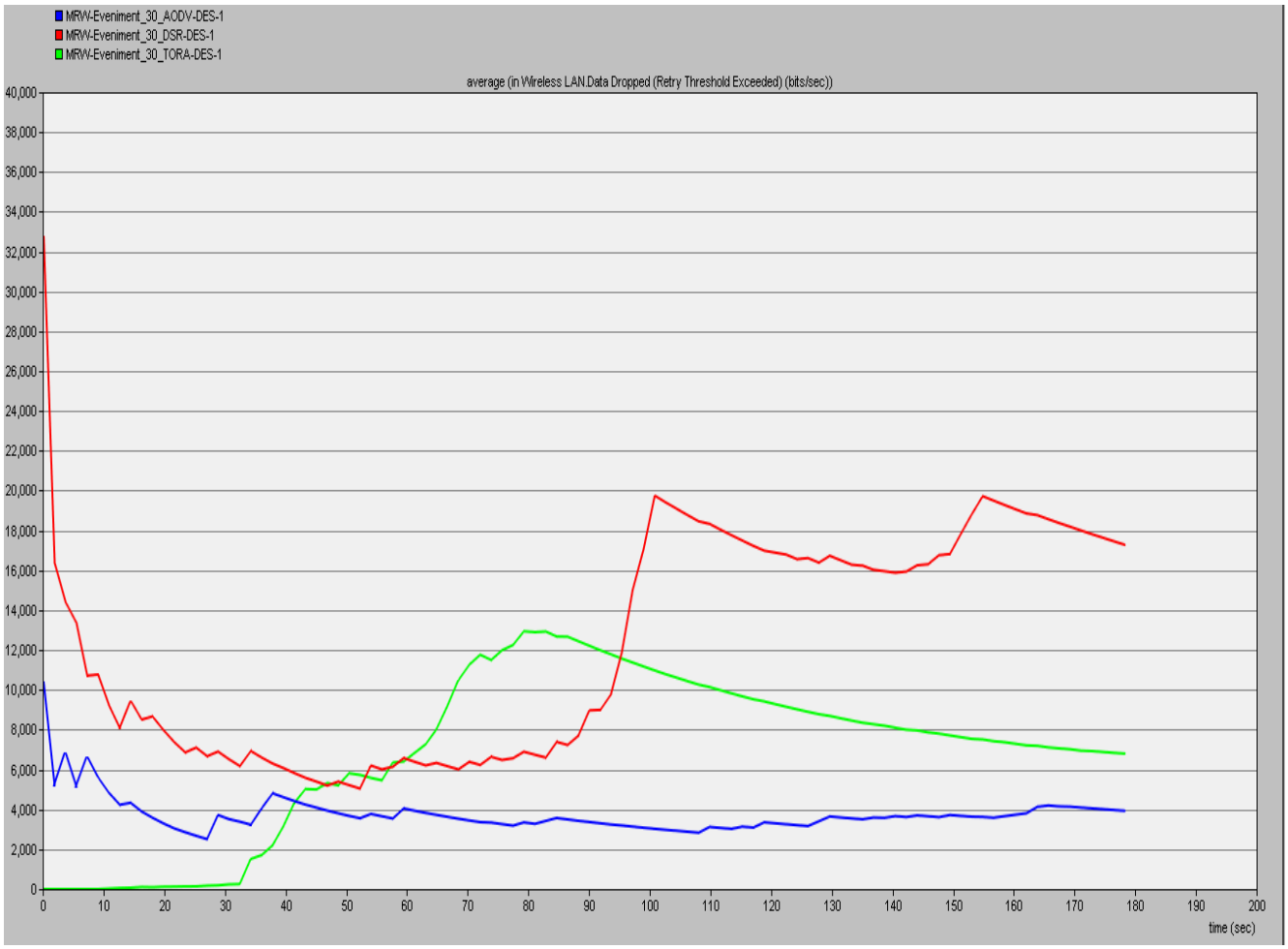

Figura 3.9 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Data Loss

Observaţie:
La fel ca şi în cazurile precedente culoarea albastră corespunde protocolului AODV, culoarea roşie protocolului DSR, iar culoarea verde protocolului TORA.

Analiza rezultatelor.

Pentru topologia cu 30 de noduri mobile observăm că numărul de pachete pierdute în cazul protocolului DSR este mai mare decât cel corespunzător AODV. Facând şi o analiză a graficului anterior observăm cum numărul de pachete pierdude depinde direct de delay. Valori mari ale delay-ului presupun creşteri ale pierderilor. Observăm aşadar cum creşterea dimensiunii reţelei a impactat performanţele protocolului DSR care prin folosirea de rute învechite cauzează atât întârzieri mai mari în reţea cât şi pierderi de pachete mai multe.
Protocolul TORA prezintă performanţe deosebite pentru prima parte a simulării, pierderile de pachete fiind aproape nule. Numărul acestora, începe sa crească pe parcurs lucru explicat datorită iniţierii unui nou proces de descoperire a rutelor.

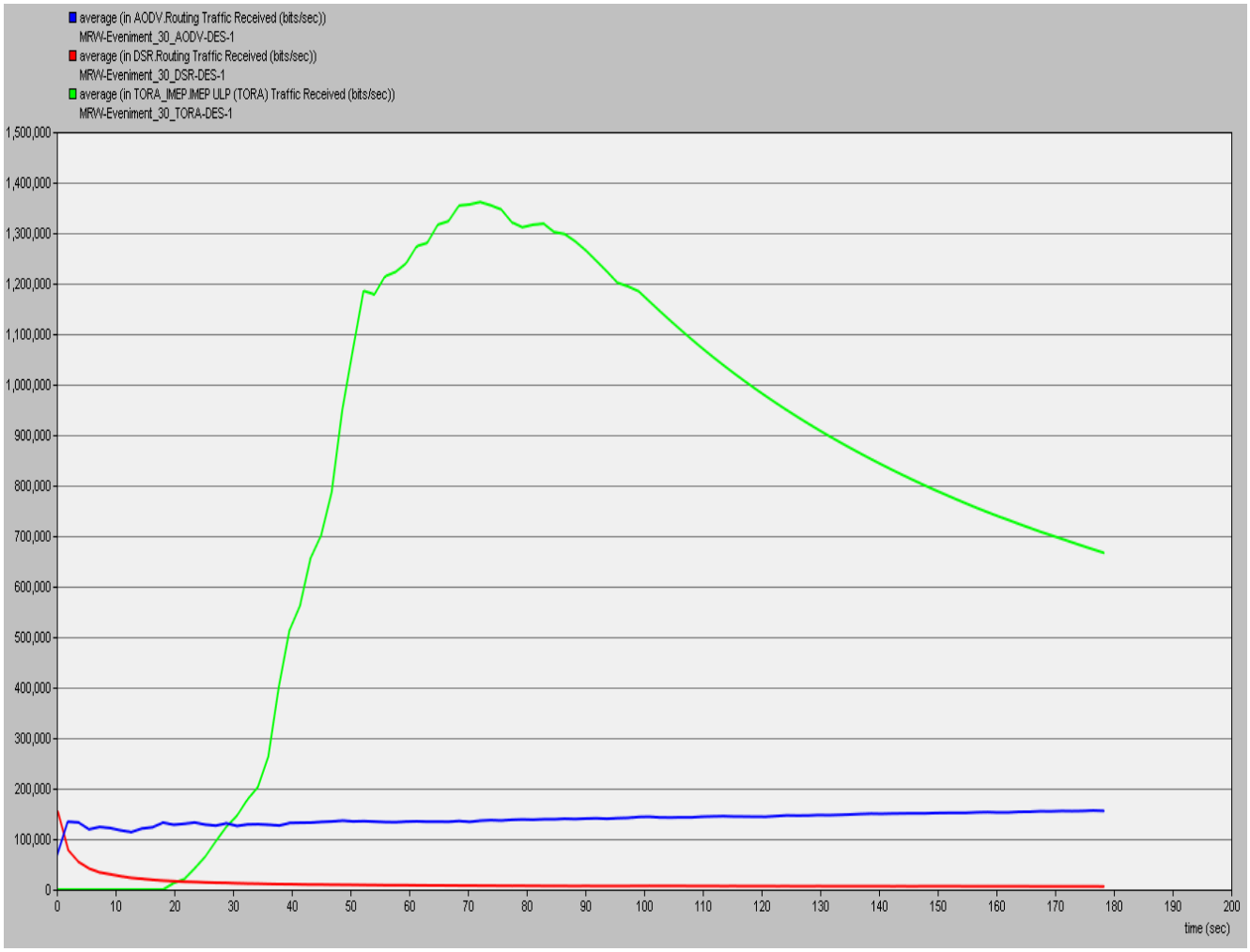

Figura 3.10 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Trafic de rutare recepţionat.

Analiza rezultatelor.

La fel ca la topologia cu 15 noduri mobile protocolul AODV transmite mult mai multe pachete de rutare faţă de DSR. Traficul de rutare recepţionat în cazul TORA se dovedeşte a fi foarte mare pentru cazul dublării numprului de noduri. Acest lucru denotă faptul că mărind dimensiunea reţelei mecansimul de găsire a rutelor folosit de TORA nu mai face faţă. Deşi AODV are un dezavantaj în ceea ce priveşte numărul de pachete de rutare transmise, performanţele în materie de throughput, delay şi data loss s-au dovedit a fi satisfăcătoare şi în mare parte mai bune decât performanţele DSR şi TORA.

3.4.1.5 Scenariul Eveniment 60 noduri

Topologia reţelei cuprinde 60 noduri mobile, dintre care 4 noduri transmit trafic FTP iar un nod recepţionează. Arhiectura acestui scenariu este prezentată în figura de mai jos:

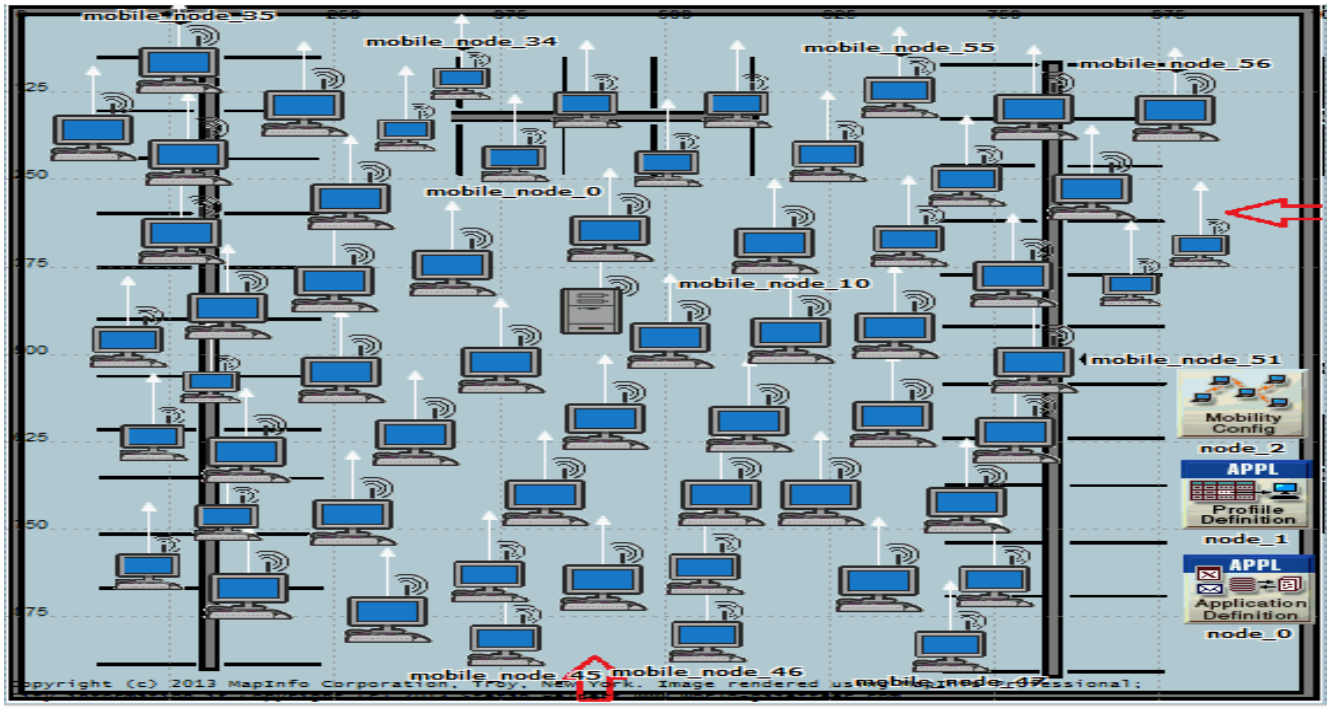

Figura 3.11 Arhitectura de reţea pentru scenariul Eveniment cu 30 noduri mobile

Rezultatele simulării

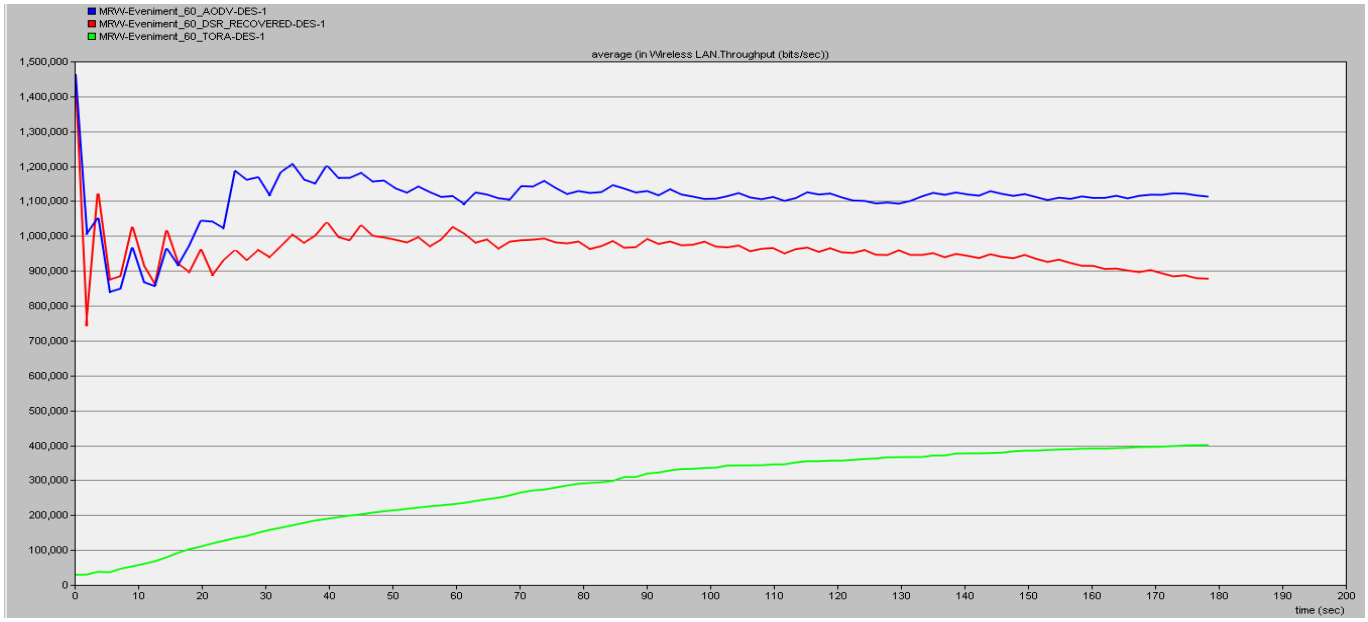

Figura 3.12 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Throughput.

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra throughput-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra throughput-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra throughput-ul protocolului TORA.

Analiza rezultatelor:

Pentru o arhitectură de reţea cu 60 de noduri mobile observăm cum AODV prezintă un throughput mai mare decât DSR. Lucru ce nu era valabil în cazul celorlalte două topologii. Protocolul DSR devine din ce în ce mai ineficient odată cu creşterea dimensiunii reţelei. Acest lucru apare, aşa cum am mai menţionat, datorită impactului pe care conservarea de rute învechite îl are. Totodată perfomanţele slabe ale protocolului TORA în ceea ce priveşte throughputul denotă faptul că mecanismul de rutare folosit de acest protocol este ineficient pentru reţele de dimensiuni mari.

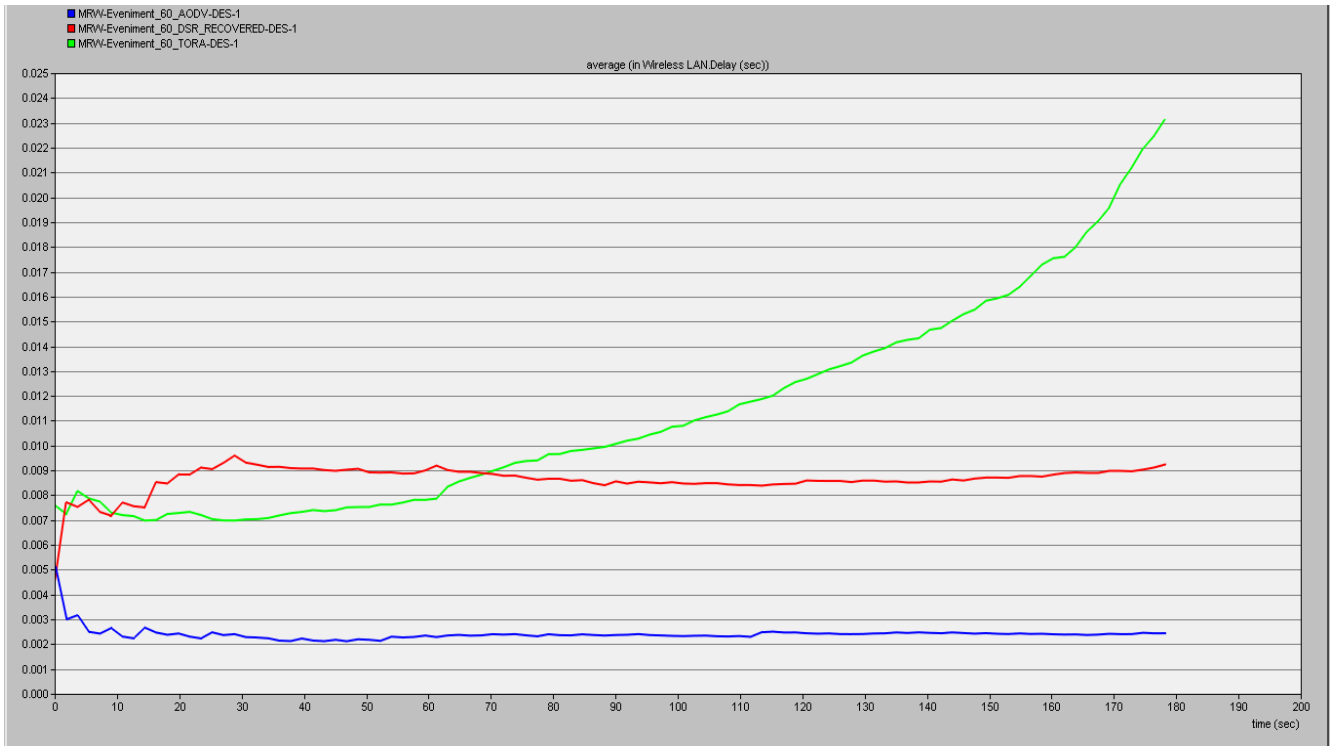

Figura 3.13 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Delay.

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra delay-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra delay-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra delay-ul protocolului TORA.

Analiza rezultatelor:

Aşa cum era de aştepat şi pentru o topologie cu 60 de noduri delay-ul corespunzător protocolului DSR este mai mare faţă de cel corespunzător protocolului AODV. Observăm cum delay-ul în cazul TORA este apropiat cu cel al DSR ba chiar are spre finalul simulării o creştere deosebită.

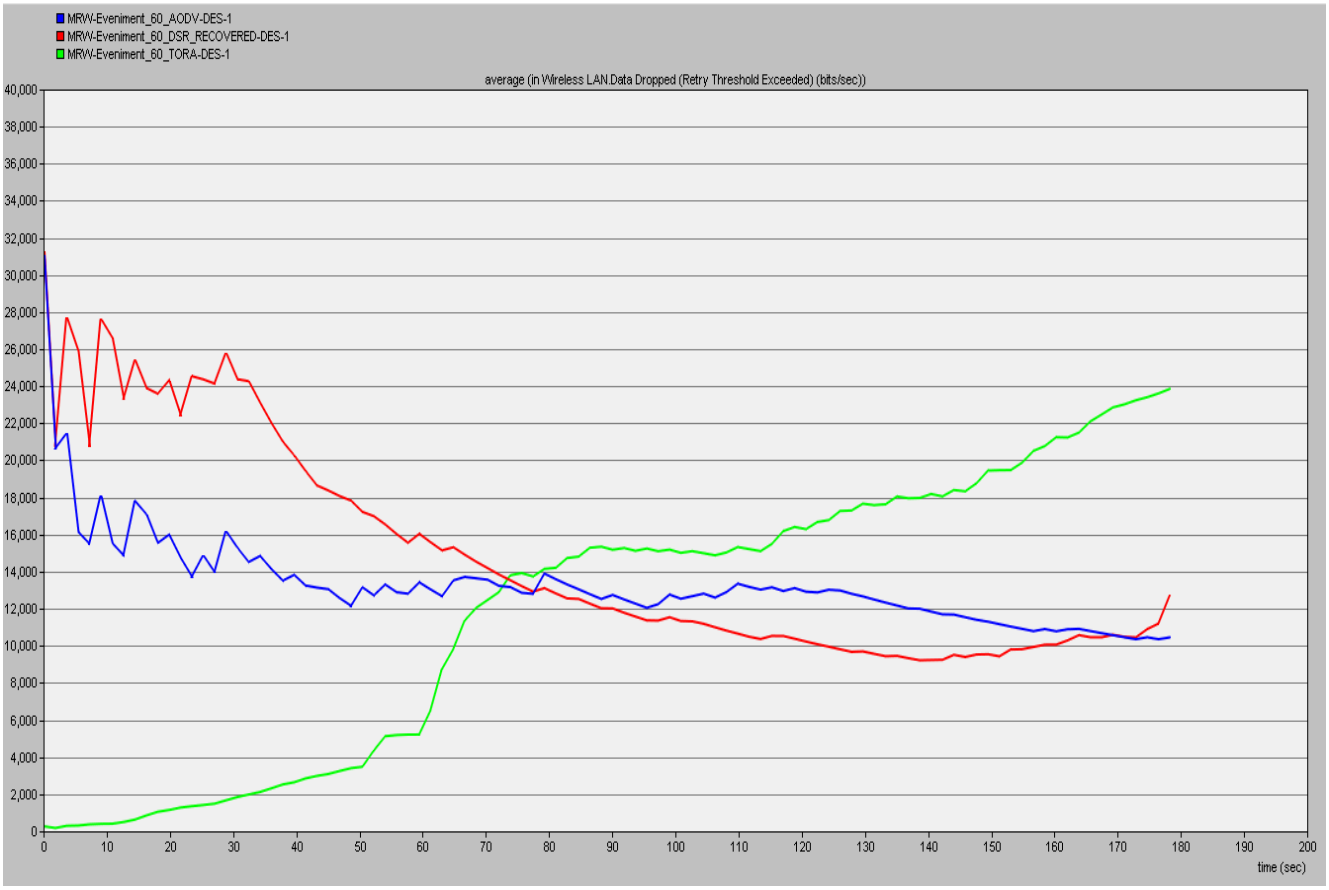

Figura 3.14 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Data Loss.

Analiza rezultatelor:

Rezultatele în acest caz sunt similare cu cele analizate în cazul precedent. Observăm că numărul de pachete pierdute în cazul protocolului DSR este mai mare decât cel corespunzător AODV şi TORA pentru prima parte a simulării. Odată ce simularea avanseayă în timp iar nodurile se aproprie pierderile scad la valori asemănătoare în cazul AODV şi DSR dar cresc în cazul TORA. Aşa cum am mai spus şi îm cazurile precedente acest fenomen este datorat iniţierii unui nou proces de descoperire a rutelor. Numărul de pachete pierdute depinde direct de delay. Valori mari ale delay-ului presupun creşteri ale pierderilor.

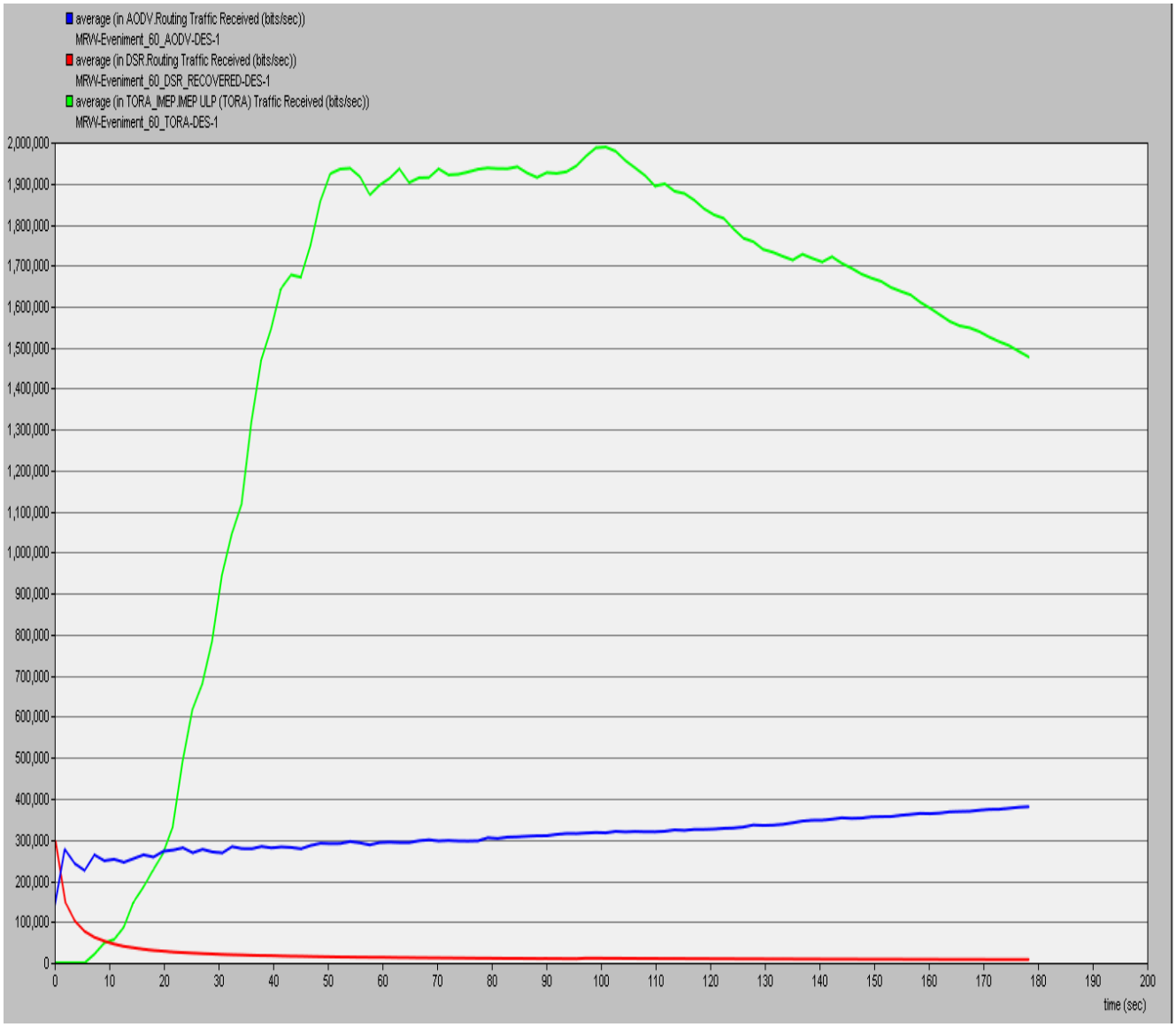

Figura 3.15 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Trafic de rutare recepţionat

Analiza rezultatelor:

La fel ca la topologia cu 30 noduri mobile protocolul TORA transmite mult mai multe pachete de rutare faţă de DSR şi AODV. AODV prezintă de asemenea un număr relativ ridicat al pachetelor de rutare transmise. Deşi acest lucru reprezintă un dezavantaj major al acestui protocol, performanţele în ceea ce priveşte throughput, delay şi data loss s-au dovedit a fi satisfăcătoare şi în mare parte mai bune decât performanţele DSR şi TORA.

Analiză finală a rezultatelor:

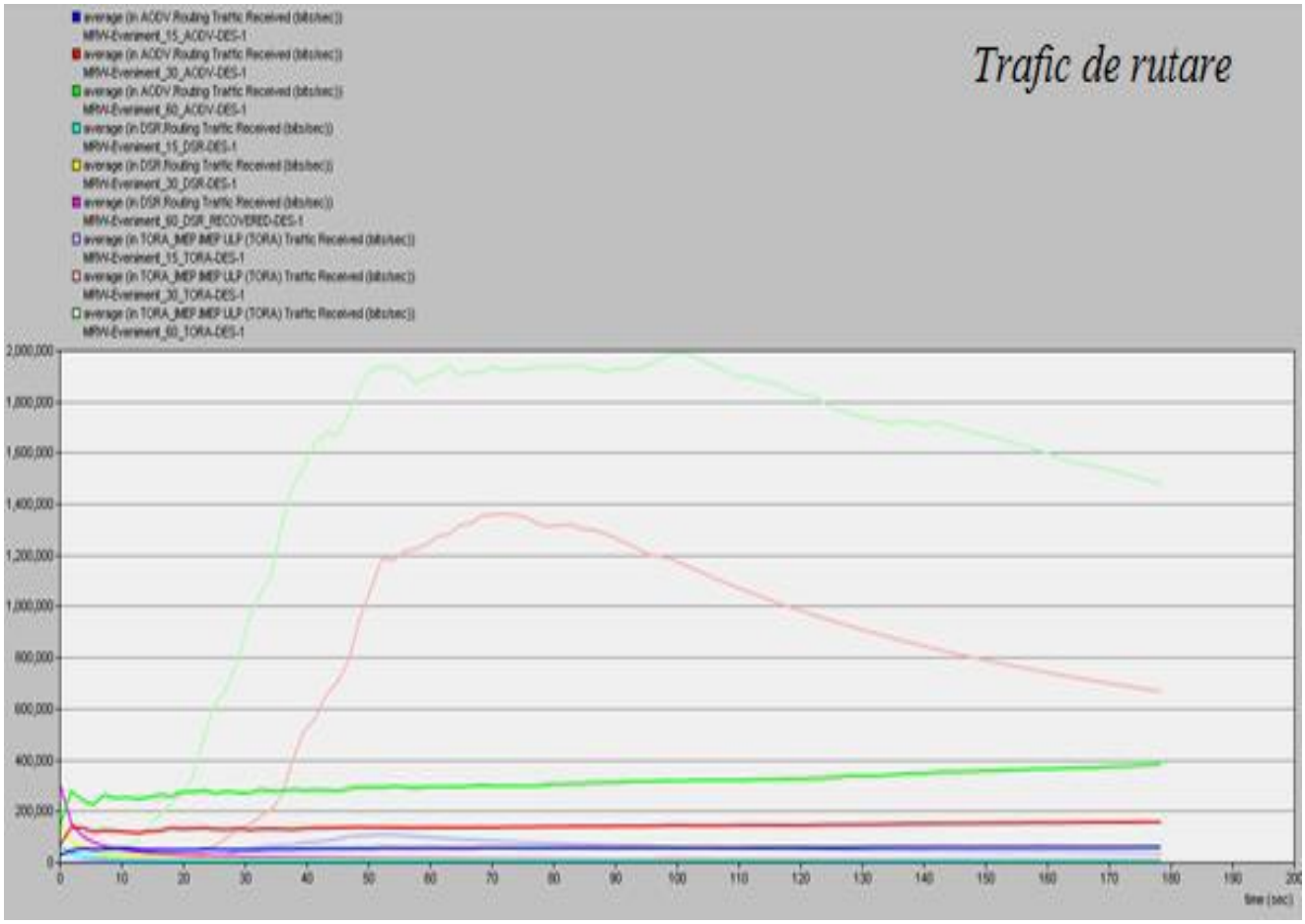

Figura 3.15 Analiza finala a traficului de rutare pentru scenariul eveniment

Legendă (Grafic Trafic de Rutare)

- Culoarea albastră corespunde protocolului AODV în cazul folosirii a 15 noduri mobile.
- Culoarea rosie corespunde protocolului AODV în cazul folosirii a 30 noduri mobile.
- Culoarea verde corespunde protocolului AODV în cazul folosirii a 60 noduri mobile.
- Culoarea bleu corespunde protocolului DSR în cazul folosirii a 15 noduri mobile.
- Culoarea galben corespunde protocolului DSR în cazul folosirii a 30 noduri mobile.
- Culoarea mov corespunde protocolului DSR în cazul folosirii a 60 noduri mobile.
- Culoarea mov deschis corespunde protocolului TORA în cazul folosirii a 15 noduri mobile.
- Culoarea roz corespunde protocolului TORA în cazul folosirii a 30 noduri mobile.
- Culoarea verde deschis corespunde protocolului TORA în cazul folosirii a 60 noduri mobile.

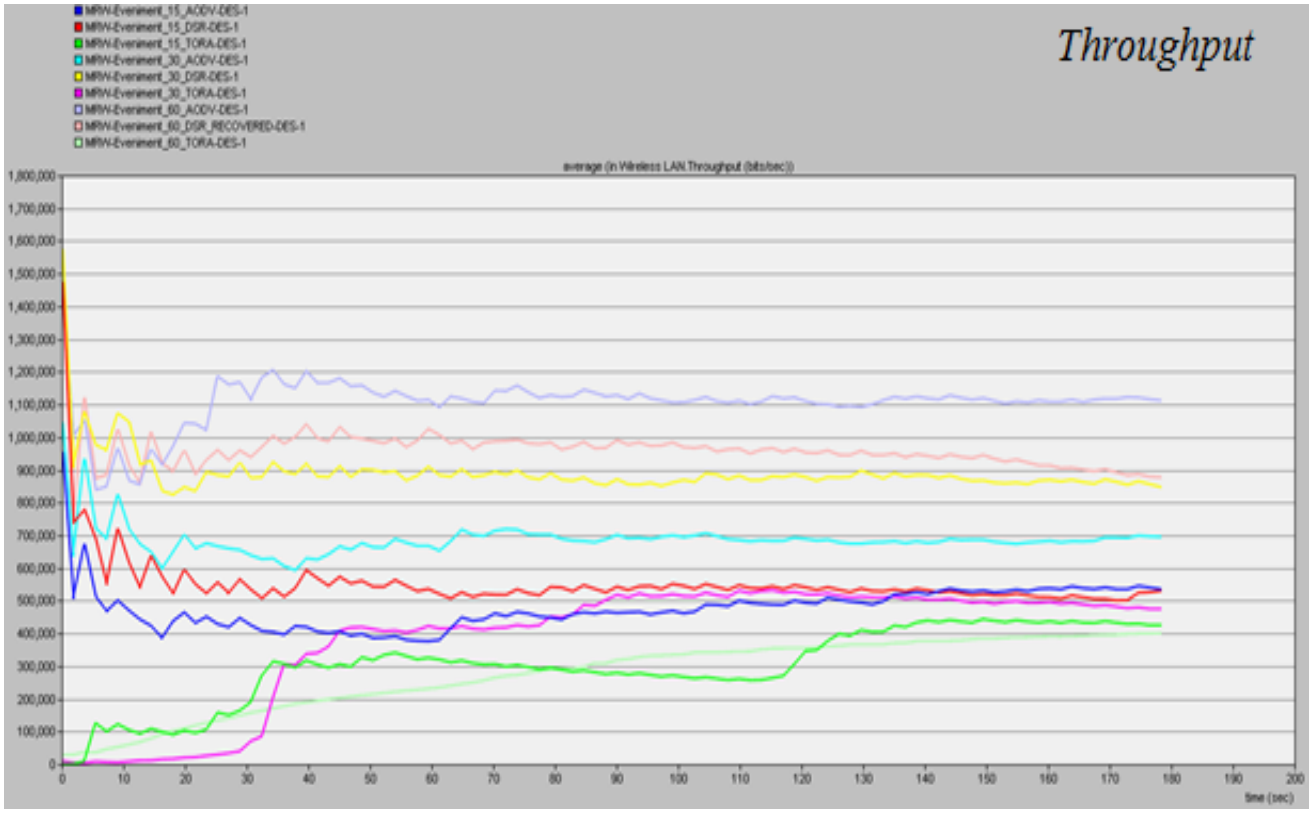

Figura 3.16 Analiza finala a throughput-ului pentru scenariul eveniment

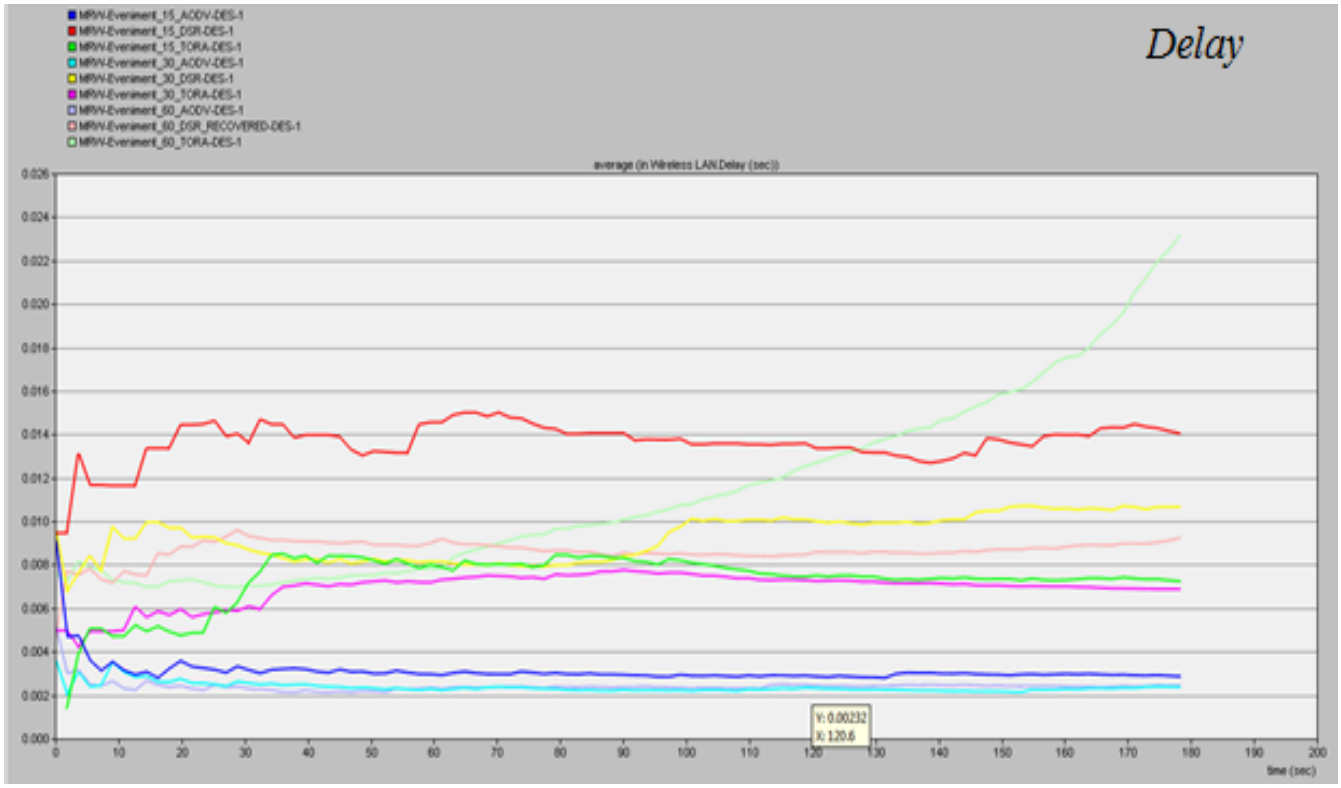

Figura 3.17 Analiza finala a Delay-ului pentru scenariul eveniment

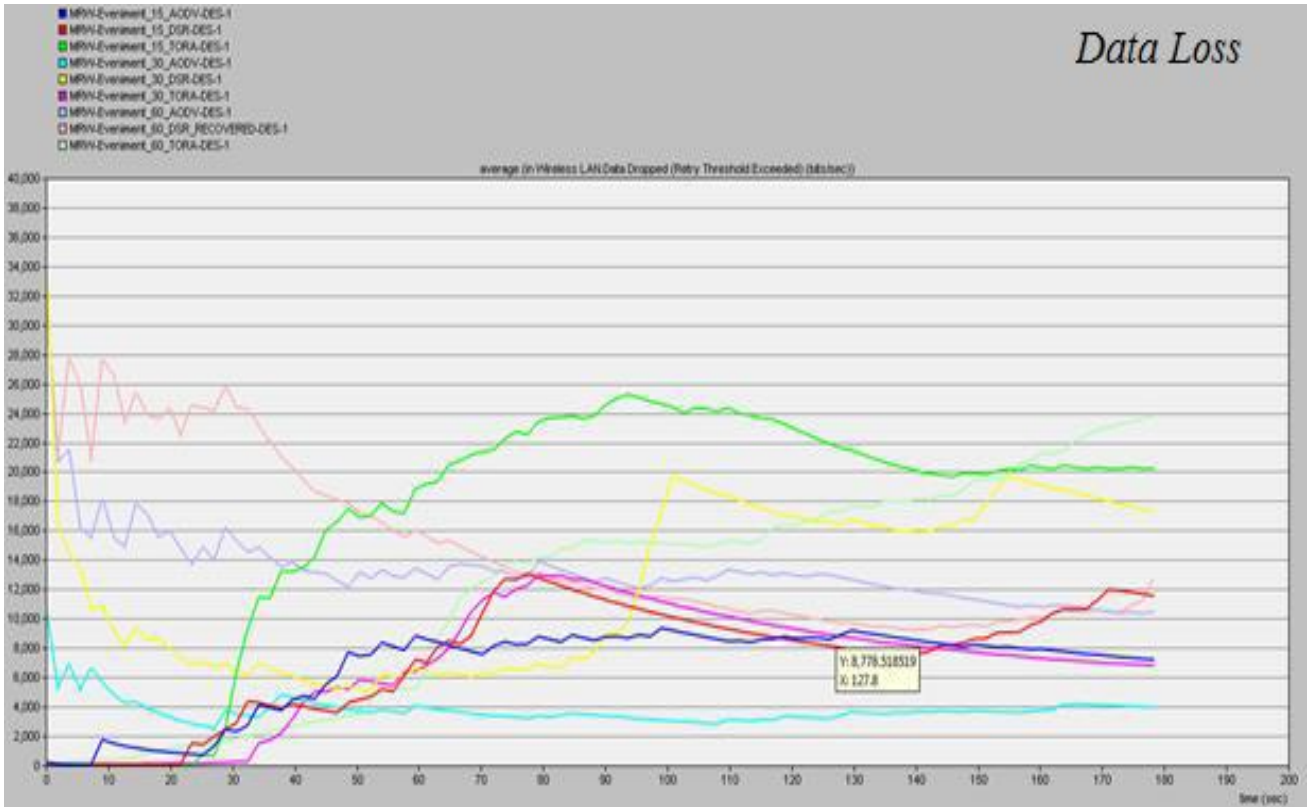

Figura 3.18 Analiza finala a numarului de pachete pierdute pentru scenariul eveniment

Legendă (Grafice Throughput, Delay şi Data Loss) .

- Culoarea albastră corespunde protocolului AODV în cazul folosirii a 15 noduri mobile.
- Culoarea rosie corespunde protocolului DSR în cazul folosirii a 15 noduri mobile.
- Culoarea verde corespunde protocolului TORA în cazul folosirii a 15 noduri mobile.
- Culoarea bleu corespunde protocolului AODV în cazul folosirii a 30 noduri mobile.
- Culoarea galben corespunde protocolului DSR în cazul folosirii a 30 noduri mobile.
- Culoarea mov corespunde protocolului TORA în cazul folosirii a 30 noduri mobile.
- Culoarea mov deshis corespunde protocolului AODV în cazul folosirii a 60 noduri mobile.
- Culoarea roz corespunde protocolului DSR în cazul folosirii a 60 noduri mobile.
- Culoarea verde deschis corespunde protocolului TORA în cazul folosirii a 60 noduri mobile.

Analiza rezultatelor.

Din graficele iulstrate observăm cum creşterea dimensiunii reţelei implică o creştere în throughput, datorită numărului mai mare de noduri intermediare, automat o creştere a numărului de pachete pierdute dar şi o creştere a traficului de rutare. Valorile pentru delay sunt destul de apropiate, acesta tinde la rândul său să crească odată cu mărirea dimensiunii reţelei.

Impactul creşterii dimensiunii reţelei asupra performanţelor celor trei protocoale este cel mai bine ilustrat la o analiază a throughput-ului. Aşa cum am observat througput-ul protocolului DSR scade comparativ cu cel al protocolului AODV atunci când numărul de noduri se măreşte. Foarte interesant de observat este faptul că throughput-ul în cazul TORA nu creşte odată cu creşterea dimensiunii reţelei. Ba chiar pentru o reţea de 60 de noduri acest parametru are valori similare cu cele pentru o reţea de 15

noduri. Acest lucru reprezintă un mare dezavantaj al protocolului deoarece indică faptul că nu poate face faţă la reţele de dimensiuni mari. Dacă pentru o reţea cu puţine noduri performanţele DSR în materie de throughput erau peste cele ale protocolului AODV, pentru o reţea de dimensiuni mai mari acest lucru nu va mai fi valabil, performanţele DSR fiind pentru reţeaua cu 60 de noduri mai slabe faţă de AODV în ceea ce priveşte throughput-ul însă mult mai bune faţă de TORA. Cele mai slabe performanţe ale protocolului DSR apar la o analiză a delay-ului. Deşi valoarea delay-ului nu este în principiu mare pentru reţele de dimensiuni mai mari cu încărcătură mai mare diferenţa de valoare se va face sigur resimţită.

Performanţele slabe înregistrate de DSR în ceea ce priveşte întârzierile şi throughput-ul sunt atribuite în mare parte utilizării agresive a cache-urilor de rute precum şi lipsa unui mecanism de expirare a rutelor învechite sau de determinare de rute noi atunci când acestea devin disponibile.
Utilizarea cache-urilor permite, însă, protocolului DSR să aibă un trafic de rutare foarte mic chiar şi atunci când numărul de noduri creşte şi reţeaua se încarcă. Acelaşi lucru se poate spune şi despre TORA unde căile multiple asigură declanşarea mult mai lenta a mecansimului de descoperire de rute. Din acest punct de vedere AODV stă foarte prost. O valoare medie a traficului de rutare recepţionat în reţeaua ad hoc cu 60 de noduri ce foloseşte ca protocol de rutare AODV ar fi 320 kbiti/sec faţă de cei 20 de kbiti/sec pe care îi înregistrează protocolul DSR în aceleaşi condiţii. Este o încărcare a reţelei de aproape 8 ori care cu siguranţă ar avea un impact şi mai mare în condiţiile unei reţele de dimensiuni mai mare.

Deşi încărcarea reţelei cu trafic de rutare reprezintă un dezavantaj major al protocolului AODV, acesta se arată totuşi a avea perfromanţe mai bune decât protocolul de rutare DSR şi decât TORA care în condiţiile creşterii dimensiunii reţelei s-a dovedit a fi din ce în ce mai puţin eficient.

3.4.2 Scenariul Zonă Devastată

Scopul urmărit.

Scopul acestei topologii este de a pune în evidenţă funcţionarea protocoalelor de rutare AODV ,DSR, TORA în cazul unei mobilităţi medii (aproximativ 6 metri pe secundă) şi un număr mic de noduri mobile (15 noduri). Am putut realiza numai conexiuni între răniţi şi serverul echipei de salvare, aflat în exteriorul clădirii în care este desfăşurată acţiunea de salvare. Salvatorii au jucat rolul nodurilor intermediare prin care a fost făcută rutarea in mediul ad-hoc de la răniţi la server.

În cazul scenariului Zona Devastată am propus o arhitectură de reţea ce replică comportamentul unei echipe de pompieri în cazul intervenţiei într-o zonă devastată. În cadrul evenimentului desfăşurat, echipa de pompieri va fi echipată cu dispozitive mobile pe care le vor utiliza cu scopul de a se organiza în acţiunea de salvare a răniţilor. Comunicaţia va avea loc folosindu-se de reţele şi protoacoalele de rutare ad hoc. În cadrul misiunii de salvare vor exista un număr de nouă pompieri exemplificaţi în cadrul exerciţiului mobil. De asemnea în cladirea în care are loc misiunea de salvare vor fi situaţi cinci răniţi de asemenea exemplificaţi in cadrul simulatorului prin noduri mobile. Răniţi vor avea aplicaţii deschise pe telefon cu ajutorul cărora vor fi găsiţi de echipa de salvare. Aplicaţiile de pe telefoanele răniţiilor transmit date în continuu, iar în momentul în care răniţii se află în raza de transmisiune a echipamentelor deţinute de către pompieri, aceştia vor putea fi reperaţi şi ajutaţi de către echipa de salvare.

Deoarece am dorit ca această simulare să fie cât mai apropriată de realitate au fost implementate trasee bine definite pentru pompieri în cadrul clădirii devastate. Această organizare a permis asigurarea unei zone cât mai mari de transmisiune şi a limitat posibilitatea pierderilor de pachete.

De asemenea, simulatorul nu mi-a permis introducerea atenuării de semnal de transmisie wireless, ce ar apărea la trecerea semnalului prin pereţii clădirii. Acest neajuns l-am simulat prin reducerea puterii de transmisiune, pentru a asigura o distanţă de transmisie de aproximativ 35 de metri. Pe harta plasată ca fundal în cadrul emulatorului sunt marcate poziţiile în care se vor opri pompierii pentru a recepţiona pachetele trimise de către dispozitivele răniţilor.
Problema care se pune, în cadrul acestui scenariu este evaluarea performanţelor celor trei protocoale de rutare specifice reţelelor ad hoc (AODV, DSR, TORA) din punct de vedere al impactului pe care îl are mobilitatea unităţilor wireless la viteze medii. În cadrul acestei topologii numărul de mobile este scazut, deoarece nu am dorit ca numărul de hopuri să aibă o influenţă decisivă asupra măsurătorilor, dimensiunea reţelei fiind doar de 15 noduri mobile.

Arhitectura de reţea pentru scenariul Zona Devastată este ilustrată în următoarea imagine. Reţeaua este alcătuită din 15 noduri mobile, dintre care 5 noduri transmit trafic către un singur nod server.

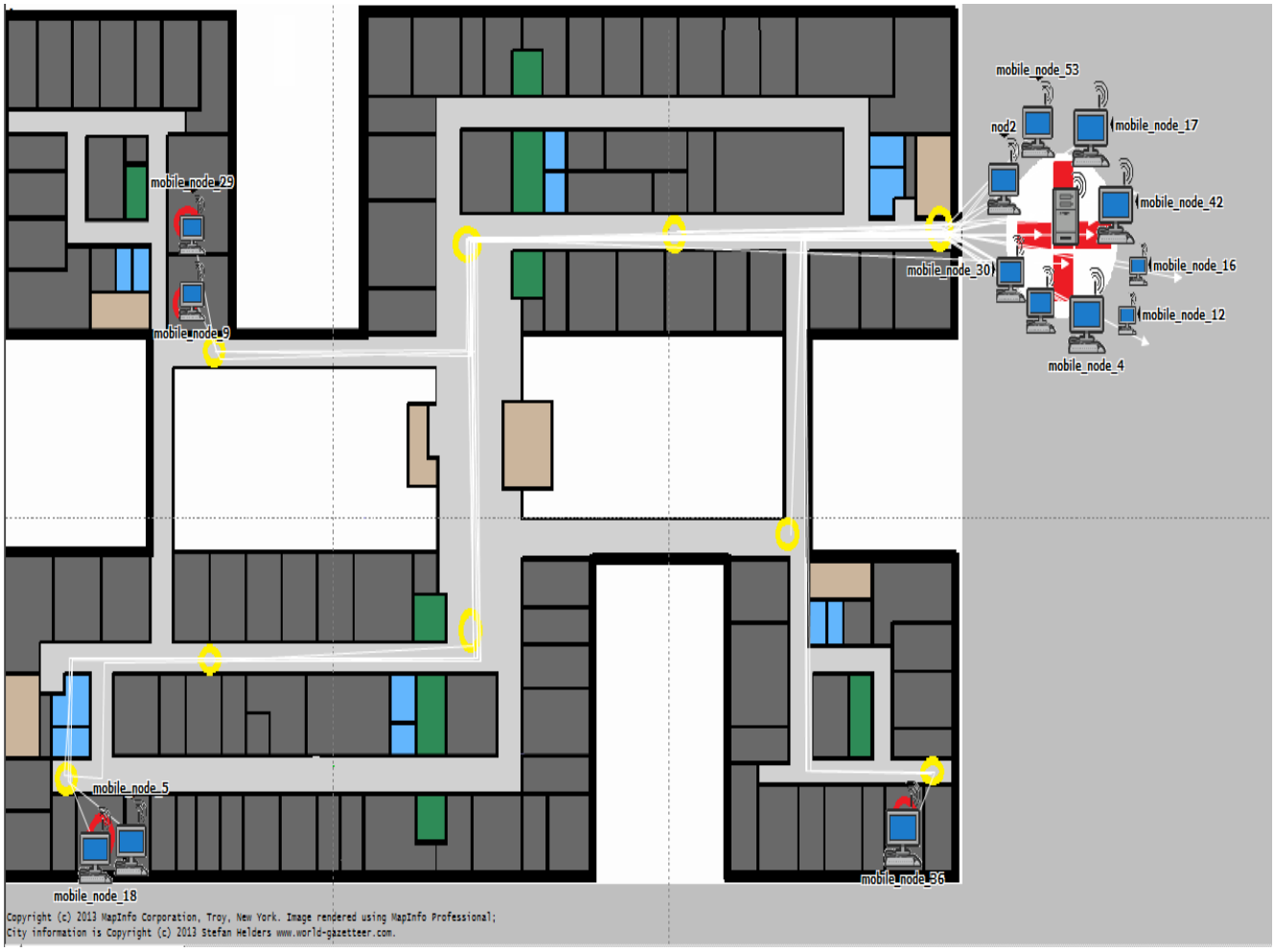

Figura 3.19 Arhitectura reţelei. Scenariul Zonă Devastată.

3.4.2.1 Detalii de implementare

Parametri configurare a reţelei.

- Parametri generali.

Parametri	
Numărul de noduri mobile	15
Protocolul de rutare	AODV,DSR,TORA
Dimensiunea reţelei (X)	120m
Dimensiunea reţelei (Y)	70m
Durata simulării	60min
Tipul de trafic	TCP
Tipul de aplicaţie	FTP
Viteza nodurilor	6 m/s

Tabel 3.8 Parametri generali

- Parametri WLAN.

Parametri	
Data Rate	11Mbps
Puterea de Transmisie	0.0000048828125W
Puterea de recepţie a datelor-prag	-95
Opţiunea CTS-to-self	Enabled
Limita Short Retry	7
Limita Long Retry	4
Intervalul AP Beacon	0.02
Max Receive Lifetime	0.5
Dimensiune Buffer	2560000

Tabel 3.9 Parametri WLAN

- Parametri FTP.

Parametri	
Command Mix	100%
Inter-Request Time	Constant(5)
File Size	Constant(50000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort(0)
Operation Mode	Serial(Ordered)
Start Time	Constant(44)
Duration	End of Simulation
Inter-repetition Time	Constant(1)

Number of Repetitions	Unlimited
Repetition Pattern	Serial

Tabel 3.10 Parametri FTP

3.4.2.2 Rezultatele

Parametri de performanţă	DSR	AODV	TORA
Throughput [kbps]	366.15	438.06	368.95
Întârzierea capăt la capăt [ms]	1.48	3.57	9.912
Traficul de rutare recepţionat	1504.779	43148.3	7612.257
Nr. pachete pierdute	9519	4376	4810

Tabelul 3.11 Parametrii de performanţă pentru scenariul zonă devastată.

În subcapitolul de faţă vor fi prezentate rezultatele simulării sub o formă grafică şi se vor ilustra o serie de indicatori de performanţă importanţi pentru analiza în cauză.
Indicatorii luaţi în calcul vor fi Throghput, Delay, Data Loss şi Traficul de rutare recepţionat. Rezultatele vor fi prezentate în paralel în cadrul aceluiaşi grafic atât pentru protocolul de rutare AODV cât şi pentru DSR şi TORA pentru a scoate în evidenţă performanţa fiecăruia dintre protocoale.

Analiza rezultatelor:

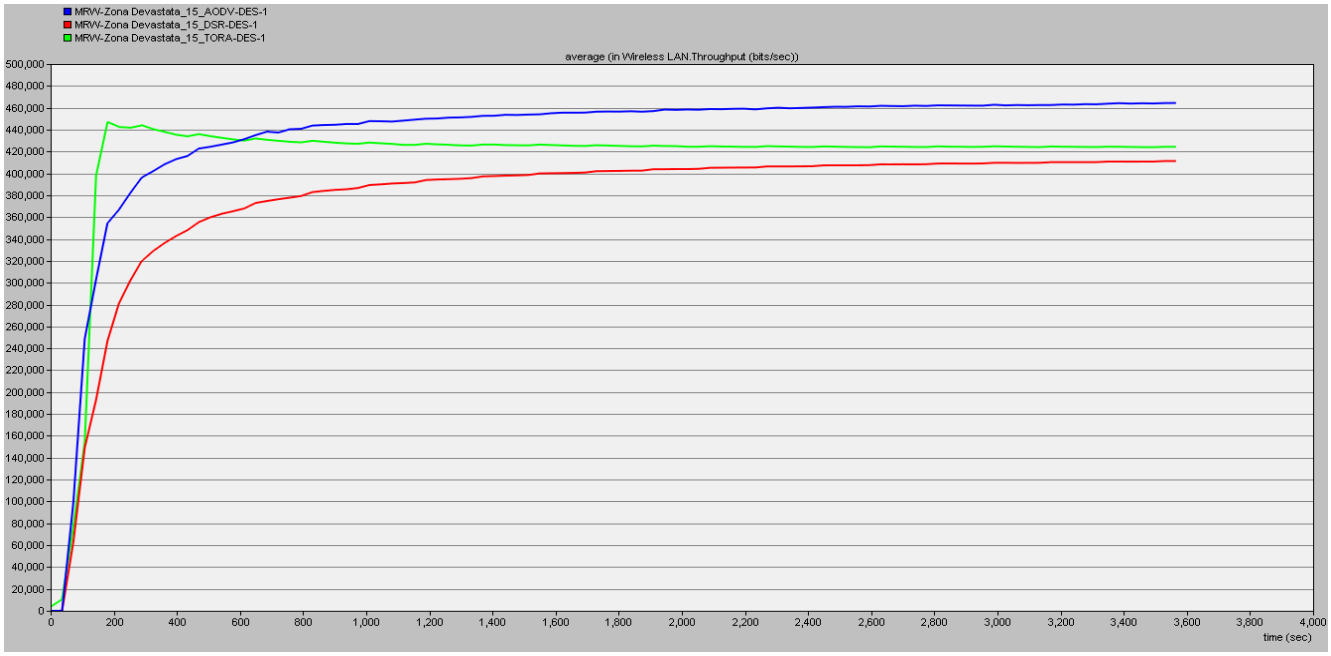

Figura 3.20 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Throughput.

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra throughput-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra throughput-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra throughput-ul protocolului TORA.

Din grafic observăm că în cazul protocolului AODV throughput-ul reţelei este în principiu mai mare faţă de cel al protocoalelor DSR şi TORA.
În cadrul acestei topologii observăm că throughputul rămâne zero pentru aproximativ 50 de secunde.

Acest lucru se întâmplă deoarece testul începe să ruleze înainte ca pompierii să ajungă în poziţiile care asigură distanţa de transmisie faţă de răniţi. Încetul cu încetul traficul va deveni mai mare cu cât mai mulţi utilizatori vor porni comunicaţia cu server-ul, ajungând ca thoughput-ul reţelei să ajungă la aproximativ 460Kbps.

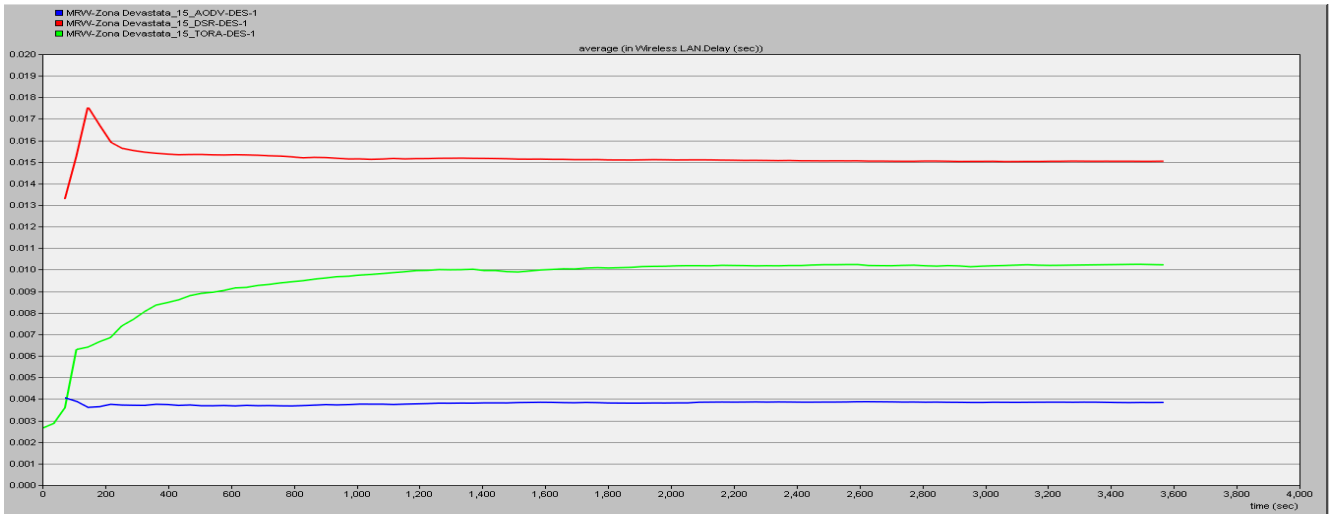

Figura 3.21 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Delay.

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra delay-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra delay-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra delay-ul protocolului TORA.

Din grafic observăm că delay-ul care apare în cazul protocolului DSR este cu mult mai mare faţă de cel corespunzător protocolului AODV dar şi faţă de TORA. Explicaţia ţine de modul în care funcţionează protocolul DSR. Acesta foloseşte rute cu un număr mai mare de hopuri faţă de cele folosite de AODV. Un număr mai mare de hopuri presupune un timp mai mare de procesare şi deci o valoare a întârzierii mai mare. Aceeşi explicaţie poate fi dată şi pentru TORA.
Sigur, întârzierea este de ordinul milisecundelor iar o diferenţă de 18 milisecunde nu ar fi remarcată de utilizatorii de date. Problema apare în cazul în care reţeaua ar fi mai mare iar numărul de hopuri până la destinaţie ar creşte. Într-o astfel de reţea protocolul DSR ar introduce rute cu o întârziere mare, făcând imposibilă utilizarea oricărei aplicaţii, mai puţin celor de transfer de date.

AODV are o întârziere foarte mică lucru explicat prin mecanismul mult mai bun de găsire a rutelor. Aşadar în acest caz protocolul AODV este mai performant decât DSR şi TORA

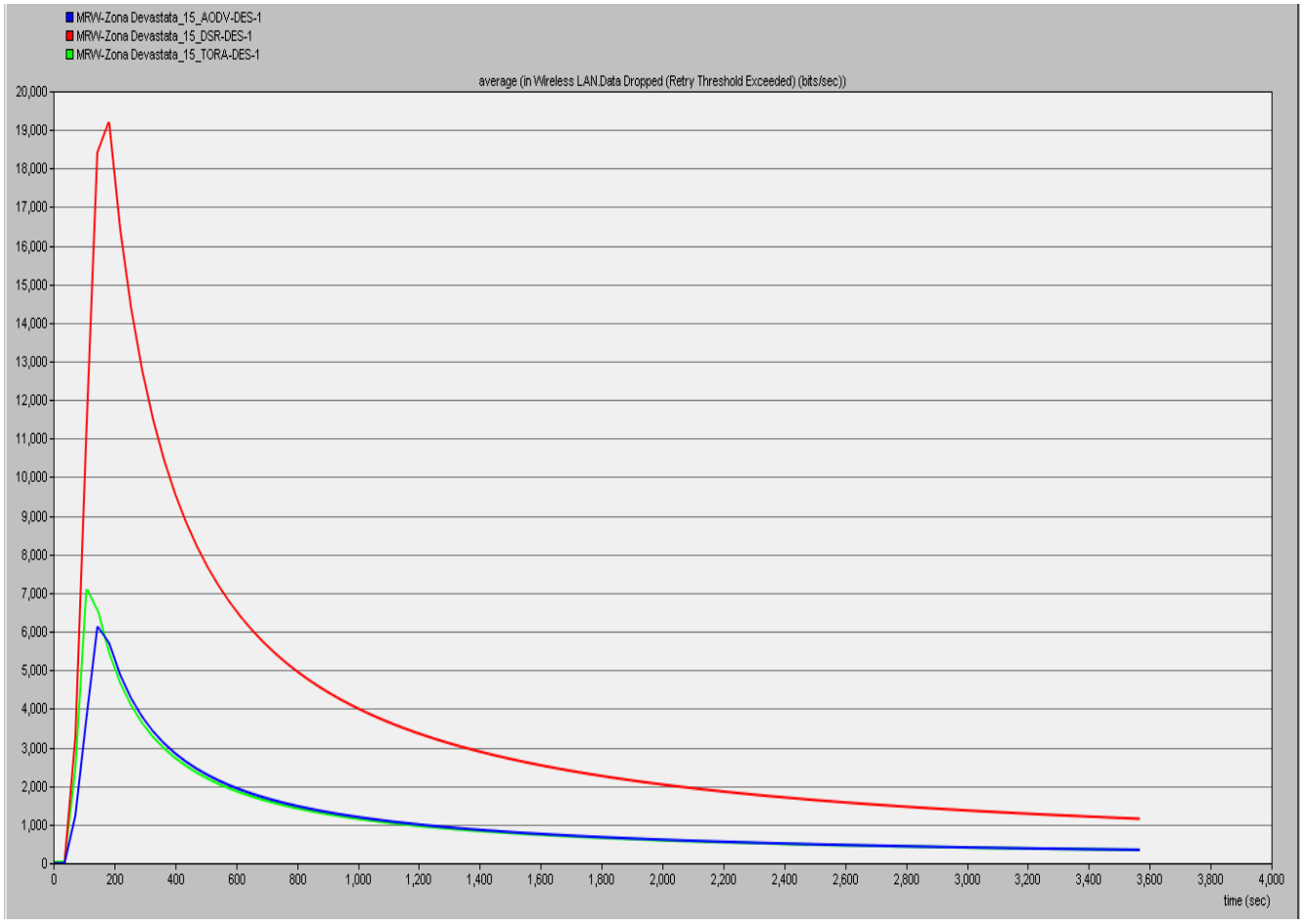

Figura 3.22 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Data Loss.

Din punctul de vedere al pachetelor pierdute protocoalele performanţa protocolului DSR este din nou contrastată de performanţa protocolului AODV dar şi de cea a protocolului TORA ce pierd catitativ mai puţine pachete decât DSR. Pierderile sunt datorate în mare parte pierderilor de rute cauzate de mobilitatea nodurilor. De asemenea, mai ales în cazul unei mobilităţi relativ mari, trebuie luat aminte faptul ca protocolul TCP corelează mobilitatea cu congestia în reţea lucru ce conduce atât la un delay mai pronunţat cât şi la pierderi.

Putem observa că la început că cele trei protocoale prezintă valori mai mari ale pierderilor. Acest moment de timp este caracterizat atât de pierderi de rute, cât şi de mobilitatea nodurilor. De asemenea observăm că pierderile scad din ce în ce mai mult, ajungând să fie apropiate către sfârşit. Această scădere apare deoarece către sfârşit mobilele ce personifică răniţii se află în apropierea serverului, iar transmia se va face direct fără a necesita intermediul unui alt nod. Faptul că la începutul simulării protocolul AODV pierde mult mai puţine pachete decât DSR se datorează mecanismului performant de rutare care deşi încarcă reţeaua cu mult trafic de acest gen, găseşte cele mai noi şi mai bune rute într-un timp scurt. Pe când DSR, pe lângă faptul că păstrează rute învechite, mai declanşează şi greu mecanismul de descoperire de rute noi fapt ce determină astfel de rezultate.

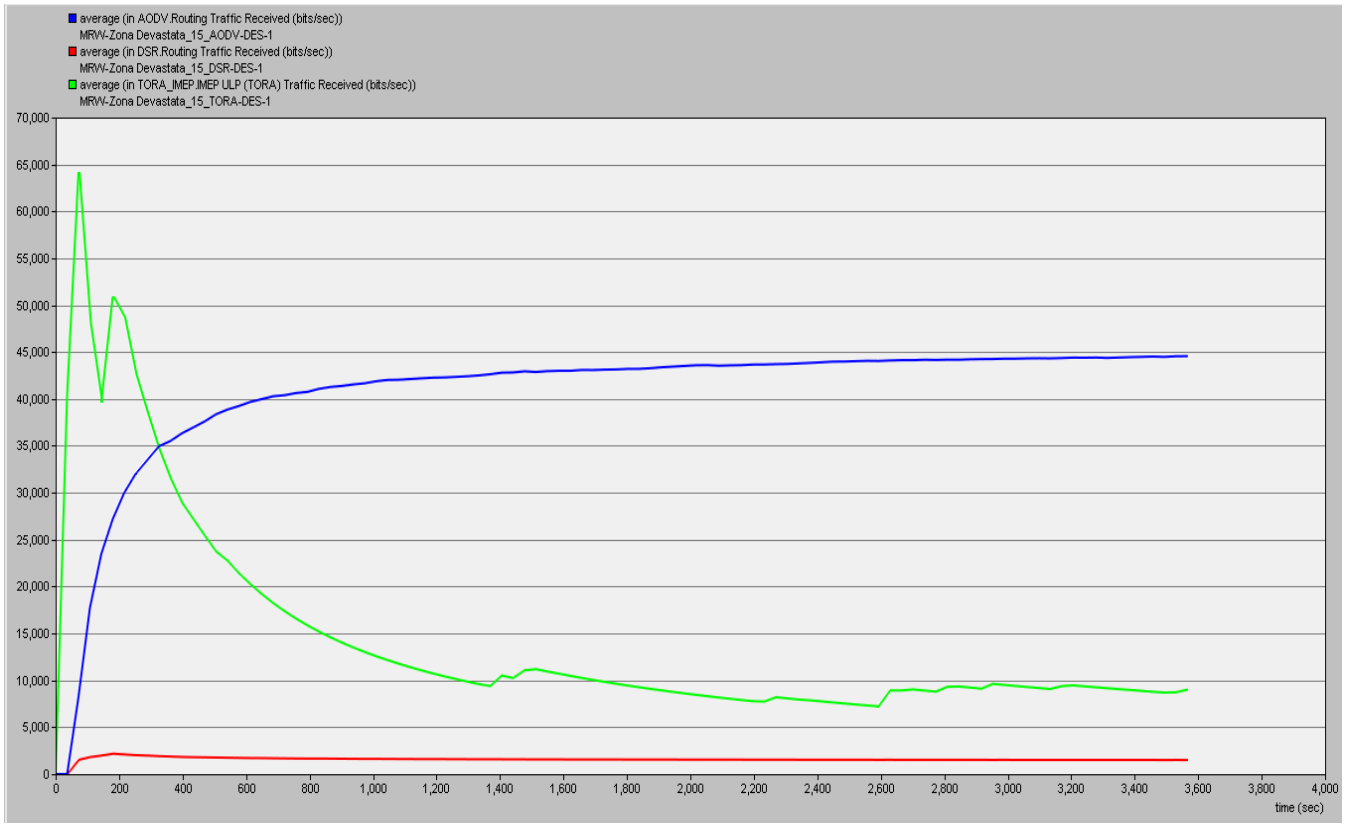

Figura 3.23 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al traficului de rutare recepţionat.

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra delay-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra delay-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra delay-ul protocolului TORA.

Analiza rezultatelor:

Aşa cum am remarcat şi la punctul precedent traficul de rutare în cazul AODV este cu mult mai mare decât traficul de rutare corespunzător DSR. Acest trafic apare datorită mişcării continue a nodurilor. Mobilitatea cauzează schimbări în topologia reţelei iar aceste schimbări cauzează declanşări ale mecanismului de descoperire de rute care inundă reţeaua cu trafic de rutare. TORA prezintă o creştere a traficului de rutarela începutul simulării când este declanşat mecanismul de rutare dar odată cu descoperirea rutelor acesta începe sa scadă şi să se stabilizeze la un nivel accesptabil.

Declanşările mecanismului de descoperire au loc foarte des în cazul protocolului AODV datorită timpilor de expirare şi mecanismului de împrospătare de rute şi rar în cazul protocolului DSR, care nu pierde aşa uşor rutele având altfel un mecanism prin care poate descoperi rute alternative fără a mai fi necesar un nou proces de descoperire de rute.

3.4.3 Scenariul Zonă de Război

Scopul urmărit

În cazul scenariului Zonă de Razboi am propus o arhitectura de reţea ce replică comportarea unor trupe de armata aflate într-un exercitiu militar. În cadrul evenimentului desfăşurat, trupele militare vor avea în posesie dispozitive mobile ce vor comunica cu un server (de asemenea mobil), folosind reţele ad hoc. În cadrul exercitiului militar vor exista cinci grupuri (A, B, C, D şi E) formate din cate trei mobile. Grupurile A,B sunt alcatuite din tancuri şi se vor deplasa cu o viteză de 36 Km/h, iar restul grupurilor care sunt alcatuite din camioane militare vor avea o viteza de deplasare de 72 Km/h (C, D, E). Scopul acestei simulări este de a testa comunicaţia dintre grupurile A şi B prin intermediul grupurilor C, D şi E utilizând protocoalele de rutare ad-hoc (DSR, AODV, TORA). Pentru toate grupurile au fost create trasee bine definite ce vor fi utilizate pentru a naviga harta.

Grupurile sunt marcate pe hartă după cum urmează: A-negru, B-rosu, C-mov, D-albastru, E-roz.

Grupurile A si B nu se vor opri deloc, urmând traseul de culoare neagră, doar grupurile C, D şi E se vor oprii pe traseu albastru, în locurile marcate cu cercuri, pentru un interval scurt de timp.

Toate grupurile sunt formate din câte 3 unităţi mobile, după cum urmează: A şi B(2 clienţi FTP şi un server FTP, având activat protocolul AODV/DSR/TORA); C, D şi E (nici un client FTP, au activat protocolul AODV/DSR/TORA). Topologia a fost gandită astfel încât conexiunile să se poată forma atât între clienţii FTP din grupul A şi serverul FTP din grupul B, cât şi între clienţii FTP din grupul B şi serverul FTP din grupul A, astfel cele două detaşamente militare transmiţând informaţii între ele.

Problema care se pune, în cadrul acestui scenariu este evaluarea performanţelor celor trei protocoale de rurtare specifice reţelelor ad hoc (AODV, DSR, TORA) din punct de vedere al impactului pe care îl are mobilitatea unităţilor wireless la viteze mari . În cadrul acestei topologii numărul de mobile este scăzut, deoarece nu am dorit ca numărul de hopuri să aibă o influenţă decisivă asupra măsurătorilor, dimensiunea reţelei fiind doar de 15 noduri mobile.

Din punct de vedere al modelării dispozitevelor mobile am considerat că o rază maximă de transimisiune de aproximativ 275 m va fi suficientă pentru a pune în vedere mecanismul de rutare.

Topologia Zonă de Război.

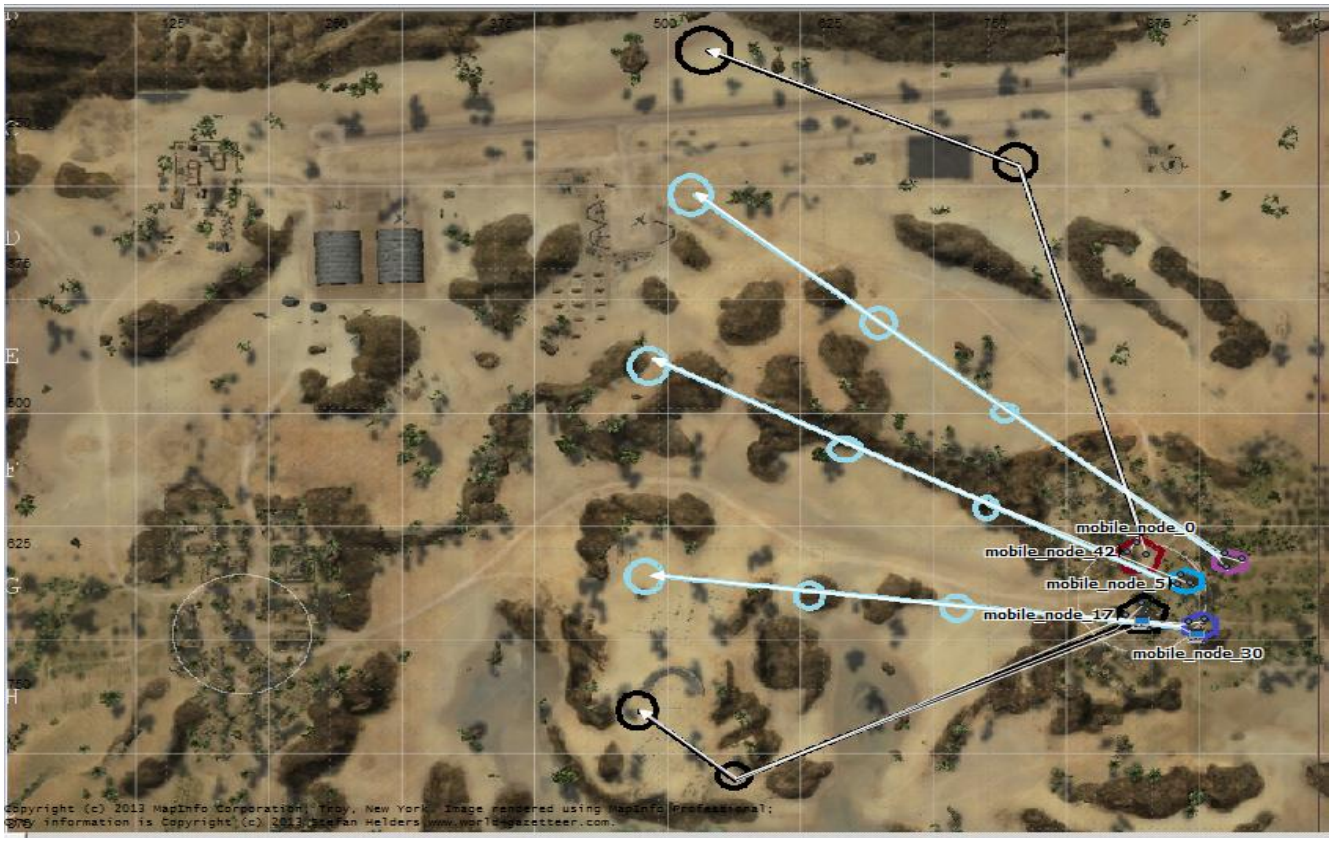

Figura 3.24 Arhitectura reţelei. Scenariul Zonă de Război.

3.4.3.1 Detalii de implementare

Parametri de configurare a reţelei:

- Parametri generali

Numărul de noduri mobile	15
Protocolul de rutare	AODV,DSR,TORA
Dimensiunea reţelei (X)	1000m
Dimensiunea reţelei (Y)	1000m
Durata simulării	60min
Tipul de trafic	TCP
Tipul de aplicaţie	FTP
Viteza nodurilor	10 m/s, 20 m/s

Tabel 3.12 Parametri generali

- Parametri WLAN.

Data Rate	11Mbps
Puterea de Transmisie	0.0003125
Puterea de recepţie a datelor-prag	-95
Opţiunea CTS-to-self	Enabled
Limita Short Retry	7
Limita Long Retry	4
Intervalul AP Beacon	0.02
Max Receive Lifetime	0.5
Dimensiune Buffer	256000

Tabel 3.13 Parametri WLAN

- Parametri FTP.

Command Mix	100%
Inter-Request Time	Constant(8)
File Size	Constant(5000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort(0)
Operation Mode	Serial(Ordered)
Start Time	Constat(0)
Duration	End of Simulation
Inter-repetition Time	Constant(1)
Number of Repetitions	Unlimited
Rpetition Pattern	Serial

Tabel 3.14 Parametri FTP

3.4.3.2 Rezultatele simulării

Parametri de performanţă	**DSR**	**AODV**	**TORA**
Throughput [Kbps]	48.203	102.51	57.33
Întârzierea capăt la capăt [ms]	8.441	2.506	4.919
Traficul de rutare recepţionat	861.8341	56531.59	6838.51
Nr. de pachete pierdute	957.84	491.17	560.84

Tabelul 3.15 Parametrii de performanţă pentru scenariul zonă de război.

În subcapitolul de faţă vor fi prezentate rezultatele simulării sub o formă grafică şi se vor ilustra o serie de indicatori de performanţă importanţi pentru analiza în cauză.

Indicatorii luati in calcul vor fi Throghput, Delay, Data Loss, Numărul de pachete de cerere, răspuns şi eroare de rută şi Traficul de rutare recepţionat. Rezultatele vor fi prezentate în paralel în cadrul aceluiaş grafic atât pentru protocolul de rutare AODV cât şi pentru DSR pentru a scoate în evidenţă capacitatea fiecăruia dintre protocoale.

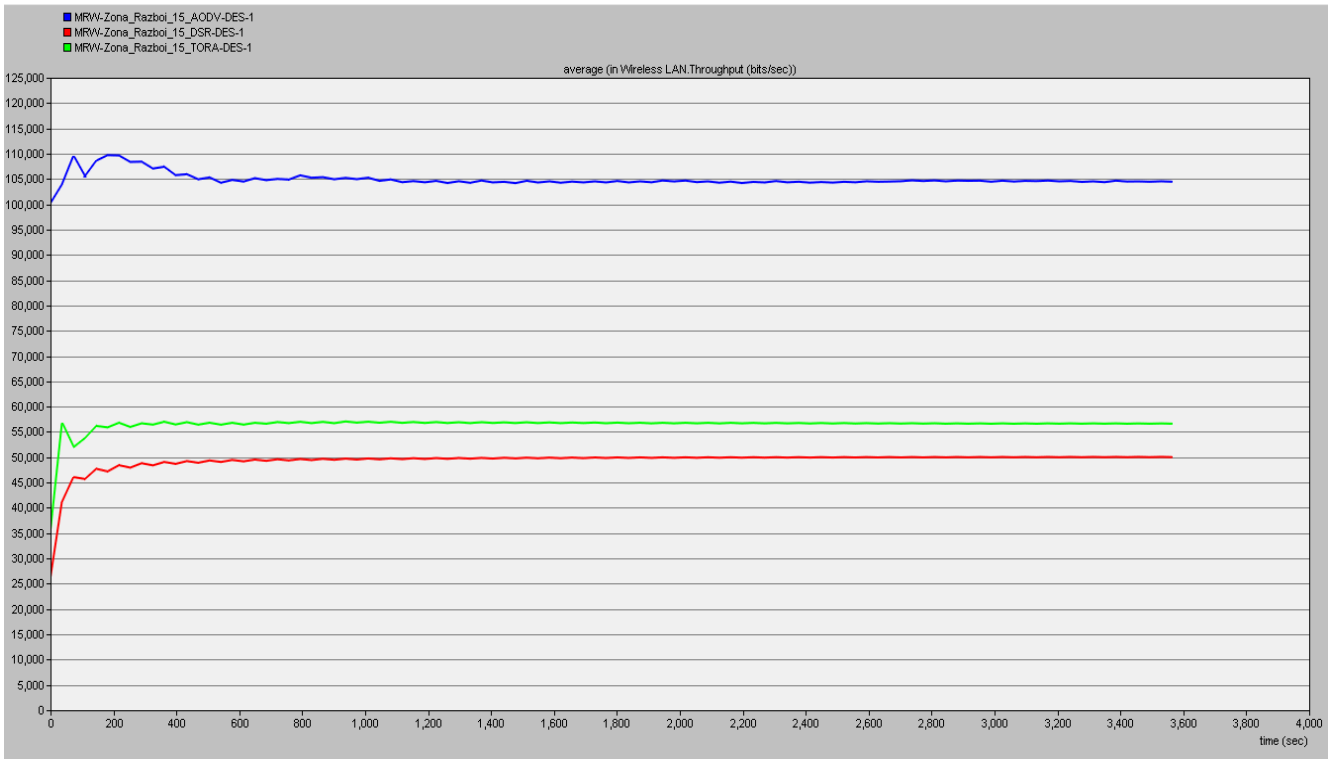

Figura 3.25 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Throughput.

Observaţii:

- Culoarea albastră a fost utilizată pentru a ilustra throughput-ul protocolului AODV.
- Culoarea roşie a fost utilizată pentru a ilustra throughput-ul protocolului DSR.
- Culoarea verde a fost utilizată pentru a ilustra throughput-ul protocolului TORA.

Analiza rezultatelor:

Din grafic observăm că în cazul protocolului AODV încărcătura reţelei este în principiu mai mare faţă de cea a protocolului DSR şi cea a protocolului TORA. Diferenţa dintre acestea nu arată cu exactitate faptul că AODV este mai perfomant, deoarece traficul de rutare în cazul AODV-ului este mult mai mare decât cel în cazul DSR-ului sau al protocolului TORA.
Valorile mari ale throughputului la începutul simulării apar datorită iniţierii schimbului de mesaje de rutare în întreaga reţea lucru ce duce la o astfel de încărcare. Pe parcursul simulării perfomanţele DSR în ceea ce priveşte throughput-ul se dovedesc a fi uşor mai crescute faţă de AODV.

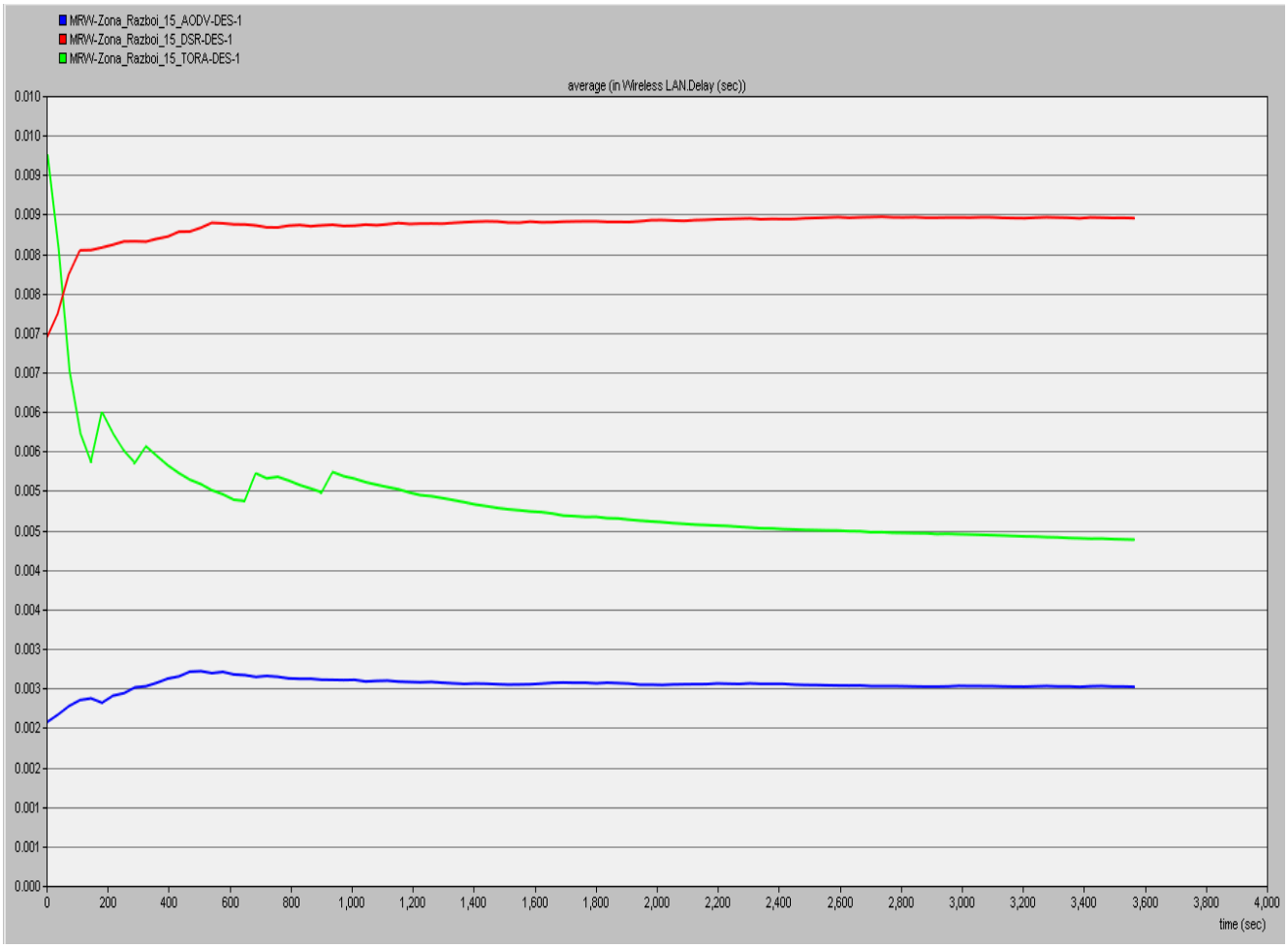

Figura 3.26 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Delay.

Analiza rezultatelor:

Graficul ne arată că delay-ul care apare în cazul protocolului DSR este cu mult mai mare faţă de cel corespunzător protocolului AODV . TORA se află undeva la mijloc. Acest fenomen apare datorită faptului că protocolul DSR foloseşte rute cu un număr mai mare de hopuri faţă de cele folosite de AODV. Un număr mai mare de hopuri presupune un timp mai mare de procesare şi deci o valoare a întârzierii mai mare.

Sigur, întârzierea este de ordinul milisecundelor iar o diferenţă de 10 milisecunde nu ar fi remarcată de utilizatorii de date. Problema apare în cazul în care reţeaua ar fi mai mare iar numărul de hopuri până la destinaţie ar creşte. Probabil ca într-o astfel de reţea performanţa protocolului DSR în ceea ce priveşte acest parametru nu ar mai fi aşa bună. AODV are o întârziere foarte mică lucru explicat prin mecanismul mult mai bun de găsire a rutelor. Aşadar în acest caz protocolul AODV este mai performant decât DSR.

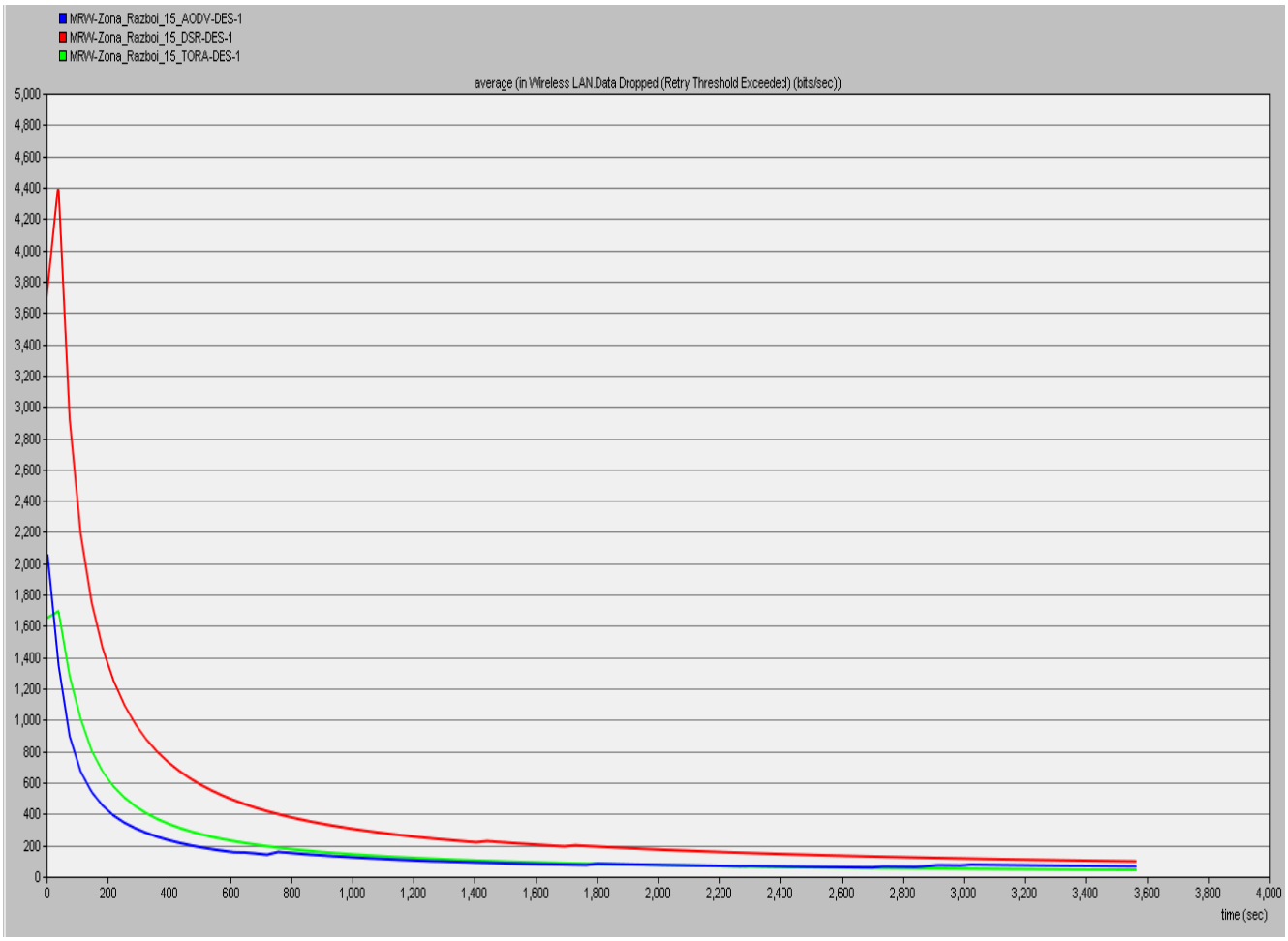

Figura 3.27 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al indicatorului de performanţă Data Loss.

Observaţie: La fel ca şi în cazurile precedente culoarea albastra corespunde protocolului AODV şi culoarea roşie protocolului DSR iar culoarea verde este asociată protocolului TORA.

Analiza rezultatelor :

Din punctul de vedere al pachetelor pierdute protocoalele prezintă performanţe asemănătoare. Pierderile sunt datorate în mare parte pierderilor de rute cauzate de mobilitatea nodurilor.
Putem observa că la început DSR prezintă valori ceva mai mari faţă de AODV şi TORA. Acest moment corespunde celui în care ruta folosită iniţial de către DSR este pierdută, iar protocolul trebuie să descopere o nouă rută către destinaţie.

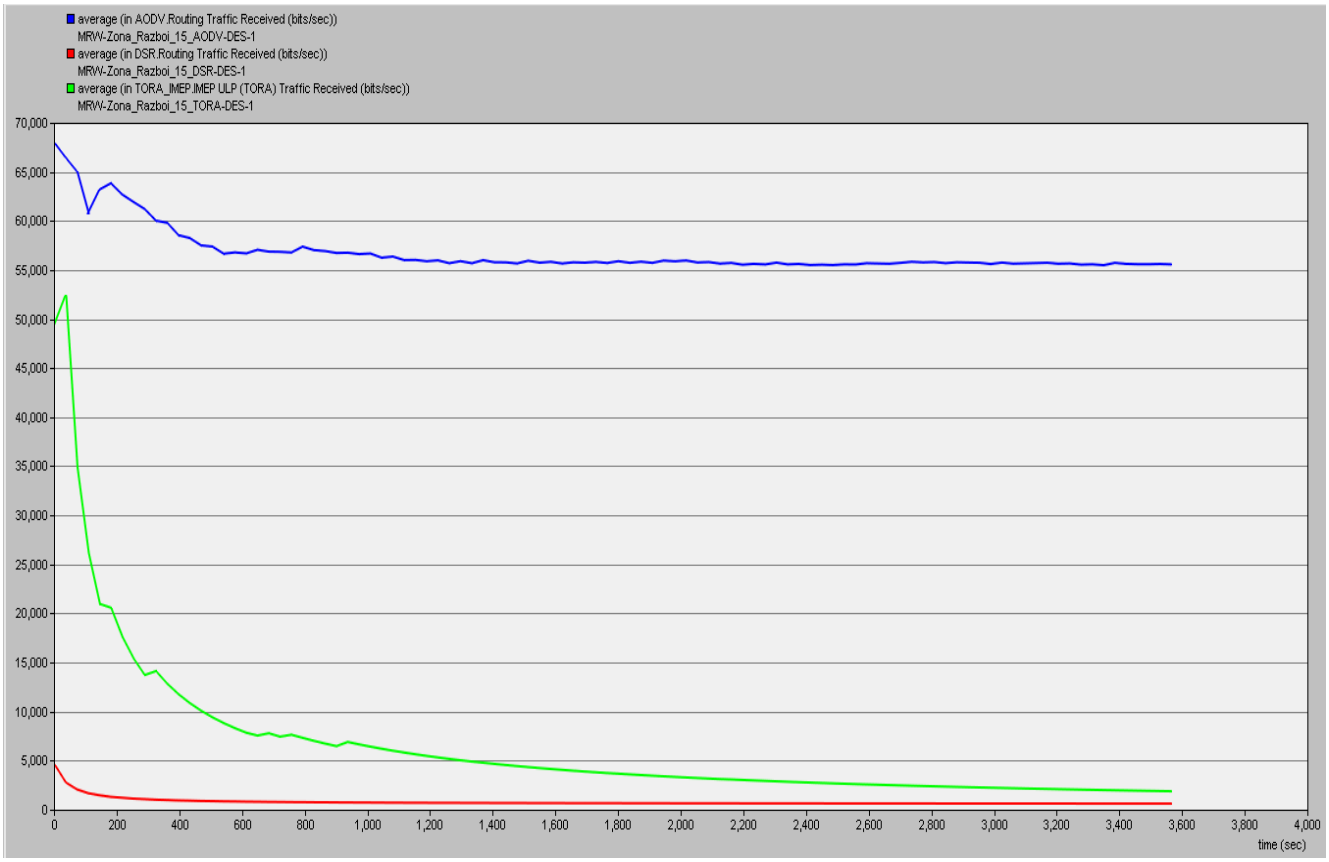

Figura 3.28 Analiza protocoalelor AODV, DSR şi TORA din punct de vedere al traficului de rutare recepţionat.

Analiza rezultatelor:

Aşa cum am mai remarcat traficul de rutare în cazul AODV este cu mult mai mare decât traficul de rutare corespunzător DSR şi TORA. Acest trafic apare datorită mişcării continue a nodurilor. Mobilitatea cauzează schimbări în topologia reţelei iar aceste schimbări cauzează declanşări ale mecanismului de descoperire de rute care inundă reţeaua cu trafic de rutare. Acest lucru se întâmplă foarte des în cazul protocolului AODV datorită timpilor de expirare şi mecanismului de împrospătare de rute şi rar în cazul protocolului DSR, care nu pierde aşa uşor rutele având de altfel un mecanism prin care poate descoperi rute alternative fără a mai fi necesar un nou proces de descoperire de rute. TORA prin mecanismul de descoperire a căilor multiple nu va declanşa la rândul său un nou mecanism de descoperire a rutelor lucru ce cauzează transmisia unui număr mic de pachete de control în reţea.

Ca o ultimă observaţie, pentru acest scenariu protocolul DSR prezintă cele mai reduse performanţe. Mobilitatea mare a nodurilor nu scalează bine cu acest protocol. Protocolul AODV s-a dovedit a fi performant şi în codiţii de mobilitate ridicată şi chiar dacă prezintă un dezavantaj în ceea ce priveşte încărcătura de rutare, se acceptă ideea ca şi de această dată să fie considerat mai bun decât DSR. În condiţiile unei mobiltăţi ridicate TORA se arată rezonabil ca performanţe.

3.5 Concluzii

În cadrul acestei lucrări am comparat performanţele protocoalelor DSR, AODV şi TORA, trei protocoale de rutare (la cerere) caracteristice reţelelor ad hoc. Cu toate că DSR, TORA şi AODV împart comportamentul (la cerere), multe din mecanismele de rutare proprii sunt foarte diferite. În particular DSR, foloseşte mecanismul de rutare a susrsei, pe când AODV foloseşte rutarea cu tabele de rutare şi numere de secvenţă. În cazul TORA, crearea rutelor se bazează pe asignarea de direcţii legăturilor, într-o reţea unidirecţională (sau sub-reţea unidirecţională), construind un graf aciclic direcţionat (DAG) cu destinaţia ca rădăcină. Am folosit modele de simulări detaliate pentru a ilustra şi evalua în paralel performanţele celor trei protocoale de rutare.

Prima parte a studiilor simulative s-a desfăşurat pentru scenarii care puneau în evidenţă impactul pe care îl are creşterea dimensiunii reţelei ad hoc asupra celor trei protocoale de rutare. Rezultatele au arătat că protocolul DSR funcţionează foarte bine în condiţii de mobilitate scăzută şi pentru dimensiuni mici ale reţelei. Protocolul de rutare AODV a avut la rândul său performanţe similare ce cele înregistrate de către DSR şi s-a dovedit a fi mai bun decât acesta în condiţii de mobilitate mică şi dimensiune a reţelei relativ mare. Performanţele TORA au lăsat de dorit în special în ceea ce priveşte throughput-ul.

A doua parte a studiilor simulative s-a desfăşurat pentru scenarii care puneau în evidenţă impactul pe care îl are creştere mobilităţii nodurilor asupra protocoalelor AODV, DSR şi TORA. În astfel de reţele performanţele protocolului AODV s-au dovedit a fi mult mai bune decât cele al protocolului DSR. TORA a avut performanţe chiar bune pentru acest scenariu şi s-a dovedit a fi mai performant decât AODV în special din punctul de vedere al încărcăturii de rutare a reţelei.

Rezultatele slabe în ceea ce priveşte întârzierea şi throghput-ul înregistrate de protocolul DSR se datorează în mare parte utilizării agresive a cache-ului de rute şi lipsei unui mecanism de împorospătarea a rutelor. Rezultatele slabe în ceea ce priveşte încărcătura de rutare înregistrate de AODV sunt datorate mecanismului de rutare care inundă reţeaua cu pachete de cerere de rută de fiecare dată când are nevoie de o rută către o destinaţie.

Consider că un mecanism de expirare a rutelor ar fi o optimizare bună pentru DSR şi ar reduce drastic delay-ul şi pierderile cauzate de folosirea rutelor învechite. O optimizare bună în cazul AODV ar fi folosirea rutării sursei, ceea ce ar conduce la o încărcătură de rutare mult mai mică.

Bibliografie:

[1] Imrich Chlamtac , Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc networking: imperatives and challenges 2003 , pag 3.
[2] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network
[3] Ian F. Akyildiz, Xudong Wang, Weilin Wang: Wireless mesh networks: a survey, "Computer Networks and ISDN Systems", v.47 n.4, p.445-487, March 2005.
[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, Security în Wireless SensorNetworks: Issues and Challenges, in: ACM, Vol. 4, Department of Computer Engg. Kyung HeeUniversity, Korea, 2006
[5] T. Lemlouma. *Le routage dans les réseaux mobiles Ad Hoc, octobre 2000.*
Université des Sciences et de la Technologie Houari Boumèdiene.
[6] Agha, K. A., Pujolle, G., Vivier. *Réseaux de mobiles et réseaux sans fil*.
Eyrolles, 2002.
[7] http://en.wikipedia.org/wiki/IEEE_802.11b-1999
[8] http://en.wikipedia.org/wiki/802.11g
[9] http://en.wikipedia.org/wiki/802.11a
[10] http://en.wikipedia.org/wiki/802.11h
[11] http://en.wikipedia.org/wiki/IEEE_802.11c
[12] http://en.wikipedia.org/wiki/802.11d
[13 http://en.wikipedia.org/wiki/802.11e
[14] http://en.wikipedia.org/wiki/802.11f
[15] Davis Srikanth V. Krishnamurthy, Ad Hoc Networks Technologies And Protocols, Edited By Prasant Mohapatra
[16] S. Basagni, I. Chlamtac, V. Syrotiuk, B. Woodward, A distance routing effect algorithm for mobility (DREAM), Dallas, TX, 1998
[17] S. Giordano, M. Hamdi, Mobility management: the virtual home region, Technical Report No. SSC/1999/037, EPFL, October 1999.
[18] Xiaoyan Hong, Kaixin Xu, Mario Gerla , Scalable Routing Protocols for Mobile Ad Hoc Networks, , Computer Science Department, University of California, Los Angeles
[19] Charles E. Perkins IBM, T.J. Watson Research Center Hawthorne, Pravin Bhagwat Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, Computer Science Department University of Maryland College Park.
[20] http://en.wikipedia.org/wiki/Link_state
[21] Eiman Alotaibi, Biswanath Mukherjee ,'' A survey on routing algorithms for wireless Ad-Hoc and mesh networks'' ,Department of Computer Science (Kemper Hall), University of California, Davis, CA 95616, USA
[22] Davis Srikanth V. Krishnamurthy, Ad Hoc Networks Technologies And Protocols, Edited By Prasant Mohapatra
[23] C. E. Perkins and E. M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In C. E. Perkins, editor, Ad hoc , Networking, pages 173-219. Addison-Wesley, 2000.
[24] C.E Perkins, E.M. Royer ,Ad-hoc on-demand distance vector routing, 1999.
[25] RFC3561
[26] Luke Klein-Berndt ''Wireless Communications Technologies GroupNational Institute of Standards and Technology" ,pag 4-6.
[27] Vincent D. Park and M. Scott Corson. "Temporally-Ordered Routing Algorithm (TORA) version 4: Functional specification". Internet-Draft, draft-ietfmanet-TORA-spec-04.txt, July 2001
[28] RFC4728
[29] M. Zapata, N. Asokan, Securing ad hoc routing protocols, Proc. ACM Workshop on Wireless Security (WiSe), 2002, 1–10
[30] http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf