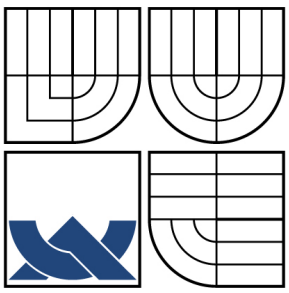
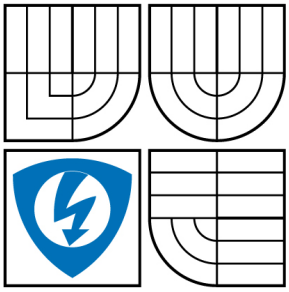


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

SMĚROVACÍ PROTOKOLY V SÍTÍCH S VOLNOU TOPOLOGIÍ

ROUTING PROTOCOLS IN SCALE-FREE TOPOLOGY NETWORKS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

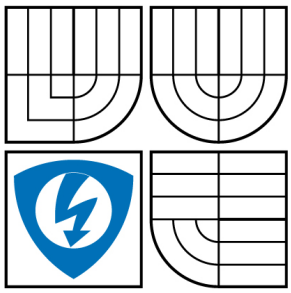
AUTOR PRÁCE — Bc. ONDŘEJ MAHDAL

AUTHOR

VEDOUCÍ PRÁCE — Ing. MICHAL SKOŘEPA

SUPERVISOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor

Telekomunikační a informační technika

Student:	Mahdal Ondřej Bc.	***ID:***	89634
Ročník:	2	***Akademický rok:***	2007/2008

NÁZEV TÉMATU:

Směrovací protokoly v sítích s volnou topologií

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou počítačových sítí s volnou topologií. Zaměřte se při tom na technologii MANET, resp. Motorola MESH. Prostudujte způsoby směrování v těchto sítích a možnosti zajištění QoS. V simulačním prostředí OPNET Modeler vytvořte model sítě MANET a implementujte v něm jednotlivé směrovací protokoly, které jsou v OPNET Modeler dostupné. Zjistěte, které protokoly jsou vhodné pro přenos multimediálních dat citlivých na zpoždění (video, hlas). V simulačním modelu implementujte i vzájemnou mobilitu uzlů.

DOPORUČENÁ LITERATURA:

[1] NOVOTNÝ, Vojtěch, Bc., Mobilní směrovací protokoly s podporou IPv6 (MANET), Diplomová práce na FEKT, VUT Brno, vedoucí diplomové práce Ing. Michal Soumar.

[2] WANG, Zheng. Internet QoS: Architectures and Mechanisms for Quality of Service, 2001

[3] OPNET Technologies, Inc OPNET Modeler Release 12 Product documentation, 2006

Termín zadání:	11.2.2008	***Termín odevzdání:***	28.5.2008

Vedoucí práce: Ing. Michal Skořepa

prof. Ing. Kamil Vrba, CSc.
předseda oborové rady

UPOZORNĚNÍ:

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Bc. Ondřej Mahdal

Bytem: Březová u Uh.Brodu 267

Narozen/a (datum a místo): 5.9.1983, Zlín

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 602 00, Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc.

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - □ disertační práce
   - ☒ diplomová práce
   - □ bakalářská práce
   - □ jiná práce, jejíž druh je specifikován jako .....

   (dále jen VŠKP nebo dílo)

Název VŠKP: Směrovací protokoly v sítích s volnou topologií

Vedoucí/ školitel VŠKP: Ing. Michal Skořepa

Ústav: Telekomunikací

Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v*:

- ☒ tištěné formě – počet exemplářů 1
- ☒ elektronické formě – počet exemplářů 1

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☒ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: 26. 5. 2008

…….. ……
Nabyvatel Autor

ANOTACE

Tématem diplomové práce (dále jen DP) je seznámení se s problematikou počítačových sítí s volnou topologií se zaměřením na technologii MANET resp. Motorola MESH. Dále studium způsobů směrování a zajištění kvality služeb QoS v těchto sítích.

Teoretická část v úvodu stručně charakterizuje vlastnosti a druhy Ad hoc sítí, další část je věnována technologii Motorola MESH a ukázce praktického využití této technologie. Rozbor problematiky zajištění kvality služeb QoS a optimalizace QoS v MANET je obsahem třetí části. Čtvrtá část specifikuje rozdělení směrovacích protokolů, rozbor směrování v MANET a charakteristiku směrovacích protokolů OLSR, AODV, DSR a TORA.

V praktické páté části je v úvodu simulována jednoduchá MANET a mesh síť, dále vytvořen model sítě MANET, do něhož jsou implementovány dostupné směrovací protokoly v simulačním prostředí OPNET Modeler a na základě simulací resp. výstupních statistik simulací jsou jednotlivé protokoly porovnány z několika hledisek a z pohledu vhodnosti pro přenos multimediálních dat (hlas, video).

Klíčová slova: Ad hoc síť, MANET, Motorola MESH, QoS, směrování, AODV, DSR, OLSR, TORA.

ABSTRACT

This master's thesis (further only MT) deal with problems of scale-free topology networks with a view to technology MANET (Mobile Ad hoc network) or more precisely Motorola MESH. Further studies routing technique and quality of services (QoS) in these networks.

Theoretic part of MT in introduction shortly characterizes properties and kind of Ad hoc networks, next part is dedicated to technology Motorola MESH and shows practical usage of this technology. Analysis of problems quality of services and optimalization QoS in MANET is content third parts of MT. Fourth part specifies division of routing protocols, analysis of routing in MANET and characteristics routing protocols OLSR, AODV, DSR and TORA.

In practical fifth part of MT are in introduction simulated simple MANET and mesh networks and further is created model of MANET network, into the model are implemented accessible routing protocols in simulation program OPNET Modeler and on the basis of simulation these protocols or more precisely output statisticians of simulation are protocols compared from several aspects and suitability for transmission of multimedia data (voice, video).

Keywords: Ad hoc network, MANET, Motorola MESH, QoS, routing, AODV, DSR, OLSR, TORA.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Směrovací protokoly v sítích s volnou topologií“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 26.5.2008 .....

(Bc. Ondřej Mahdal)

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce Ing. Michalu Skořepovi, za velmi užitečnou metodickou pomoc, neúnavné vedení práce, obsahové nasměrování textu práce, řadu podnětných rad a zkušeností. V neposlední řadě pak za ochotu ke konzultacím a cenné rady při zpracování práce. Dále bych touto formou velmi rád poděkoval svým rodičům, bratrovi a své přítelkyni za jejich maximální podporu v průběhu studia.

V Brně dne 26.5.2008 .....

(Bc. Ondřej Mahdal)

SLOVNÍK POJMŮ A ZKRATEK

Ad hoc – Dočasné spojení mezi rovnocennými prvky.
AODV – *Ad hoc On Demand Distance Vector Protocol* – Reaktivní směrovací protokol.
Best effort – Způsob zacházení s pakety, který využívaly starší síťové technologie a který neposkytuje žádné garance.
Broadcast – Všesměrové vysílání.
DARPA – *The Defense Advanced Research Projects Agency* – Výzkumné oddělení amerického ministerstva obrany.
DiffServ – *Differentiated Services* – Způsob zajištění QoS, který dělí síťový provoz do několika málo tříd.
DSCP – *DiffServ Code Point* – DSCP je 6 bitová hodnota části DS pole, což je dnešní název pro bývalý ToS Byte a využívá se pro označení požadovaného způsobu zacházení pro každý paket.
DSR – *Dynamic Source Routing* – Reaktivní směrovací protokol.
FQMM – *Flexible QoS Model for MANET* – První model QoS navržený pro MANET síť.
Full mesh – Plně propojená síť mesh, kde komunikují uzly každý s každým.
***HELLO* zpráva** – Používá se pro zjišťování sousedů.
IntServ – *Integrated Services* – Způsob zajištění QoS, který rozlišuje každý datový tok na základě identifikátoru. Používá se ve spojitosti s protokolem RSVP.
MANET – *Mobile Ad hoc Network* – Systémy mobilních stanic, které se dovedou sami-organizovat a fungovat v dočasné síti s proměnnou topologií.
MEA – *Motorola Enable Access* – Koncept založený na Motorola MESH architektuře.
Mesh – Bezdrátová síť bez centrálního prvku.
Motorola Multi-Hopping – Technologie, která umožňuje, aby klient mohl vystupovat jako router/repeater a dovoluje vícenásobné skoky mezi uzly.
MPR – *Multi-point relays* – Uzel v OLSR, který zjednodušuje topologii a omezuje množství režijních informací.
OLSR – *Optimized Link State Routing Protocol* – Proaktivní směrovací protokol.
On-demand směrování – Směrování je zahájeno pouze v případě vzniklého požadavku.
Partial mesh – Částečně propojená síť mesh.
PCMCIA – *Personal Computer Memory Cards International Association* – Je rozšiřující slot, vyskytující se především v noteboocích.
Peer-to-peer – P2P sítě – Jsou sítě, kde spolu komunikují přímo klienti na rovnocenné úrovni. Opak klient-server.
Přístupový bod – *Access point* – Je uzel v bezdrátové síti, ke kterému se připojují klienti.
PSTN – *Public Switched Telephone Network* – Standardní telefonní síť.
QMPR – *QoS Multi-point relays* – Obdoba MPR u OLSR.
QOLSR – *QoS OLSR* – Rozšíření protokolu OLSR o podporu QoS.
QoS AODV – Rozšíření protokolu AODV o podporu QoS.
QoS – *Quality of Services* – Definice požadavků na poskytovanou službu.
RERR zpráva – *Route Error zpráva* – Chybová zpráva, generovaná uzlem např. při výpadku jednoho ze sousedních uzlů.

RFC – *Request For Comments* – Dokument vydaný IETF upravující určitou oblast. Může jít o standard nebo informační text.
RREP zpráva – *Route Reply zpráva* – Je odpovědí na RREQ zprávu, jestliže uzel zná cestu k cíli, nebo on sám je cílem.
RREQ zpráva – *Route Request zpráva* – Používá se v případě, když jeden z uzlů chce poslat data jinému uzlu, který není jeho soused.
RSVP – *Resource ReSerVation Protocol* – Protokol využívá cílová stanice, která očekává určitá data a chce si pro ně zajistit zaručený průchod sítí.
Směrovač – *Router* – Síťový prvek třetí vrstvy IP protokolu.
Soft QoS – Dovoluje selhání QoS, například při ztrátě cesty, nebo rozdělení sítě.
Soused – *Neighbor* – Sousední uzel.
***TC* zpráva** – *Topology Control* – Používá ji protokol OLSR ke zjištění stavu jednotlivých linek.
TORA – *Temporally-Ordered Routing Algorithm* – Adaptivní směrovací protokol.
ToS – *Type of Services* – Pole v IP datagramu, které specifikuje typ služby.
Uzel – *Node* – klient + router.
WiFi – *Wireless Fidelity* – Bezdrátové síťové prvky pracující dle standardu 802.11x.
Zpětný kanál – *Backhaul* – Je kanál sloužící pro zpětnou komunikaci.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

Úvod

Dnešní doba je charakteristická tím, že ve všech oblastech lidského počínání roste význam internetu a obecně nutnosti mít k dispozici aktuální informace a vysokorychlostní přenos dat prakticky kdykoliv a kdekoliv. Z tohoto pohledu je tedy velmi zajímavé zabývat se mobilními Ad hoc sítěmi (MANET), kde každé bezdrátové komunikační zařízení (uzel) může být umístěno prakticky kdekoliv a několik takových uzlů tvoří autonomní systém, který může vystupovat zcela samostatně, nebo může být připojen do internetu či fixní sítě.

Zajímavou koncepci, která vychází z MANET vyvinula firma Motorola pod názvem Motorola MESH, kde koncové stanice podobně jako u MANET vystupují jako základnové stanice, čímž je opět docíleno velké variability sítě. Praktické využití těchto sítí bylo v první fázi pro vojenské účely, ale v současnosti se již využívají i pro veřejné účely a jejích využití bude v následujících letech stoupat. Například v městě Cocoa Beach na Floridě v USA ji využívá místní policie pro přenos real-time videa ze svých automobilů. Síť tedy musela být optimalizována pro určitou žádanou propustnost. Tedy i z tohoto pohledu je MANET resp. Motorola MESH perspektivní a s praktickou implementací se budeme setkávat čím dál častěji.

Tématem diplomové práce je seznámení se s problematikou počítačových sítí s volnou topologií se zaměřením na technologii MANET resp. její implementaci v podobě Motorola MESH. Dále studium způsobů směrování a zajištění kvality služeb QoS v těchto sítích. Následně seznámení se simulačním prostředím OPNET Modeler a implementace dostupných směrovacích protokolů do vytvořeného modelu MANET sítě.

První část DP obsahuje stručnou charakteristiku Ad hoc sítí s uvedením druhů Ad hoc sítí, jejichž vlastnosti a charakteristika jsou uvedeny v dalších kapitolách.

Další část teoreticky rozebírá Motorola MESH sítě, uvádí stručně historii vývoje této technologie, dále význačné vlastnosti určující charakter technologie a v neposlední řadě také výhody. Na závěr této části jsou uvedena tři praktická řešení Motorola MESH sítě.

Úvod třetí části je věnován obecně problematice QoS, rozboru jednotlivých modelů zajištění QoS s uvedením stručné charakteristiky. Poté je diskutována problematika optimalizace QoS v MANET, kde jsou zmíněny problémy vyplývající z vlastností těchto síti, které nepříznivě ovlivňují zajištění QoS.

Čtvrtá část v úvodu specifikuje rozdělení směrovacích protokolů do skupin dle jejich vlastností. Následuje rozbor problematiky směrování v MANET, charakteristika jednotlivých směrovacích protokolů a u protokolů AODV a OLSR je uvedeno i jejich rozšíření pro podporu QoS.

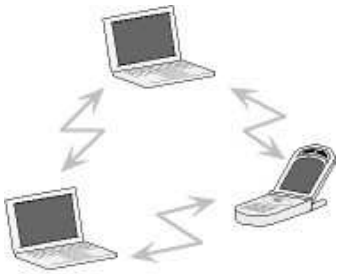
Poslední pátá část DP popisuje vytvoření modelu sítě MANET v OPNET Modeleru s uvedením stručné charakteristiky jednotlivých použitých komponent a parametrů, které byly nastavovány. Simulováno bylo celkem pět scénářů, z nichž čtyři obsahují implementaci jednotlivých protokolů, a na posledním pátém je ilustrován výpadek několika uzlů. Na obrázcích je také ukázáno směrování dat pro jednotlivé protokoly. Poslední kapitola páté části obsahuje porovnání protokolů z několika hledisek a uvedení výstupních statistik simulace.

Závěr shrnuje zjištěné poznatky a popisuje vhodnost jednotlivých směrovacích protokolů pro přenos multimediálních dat.

1. SÍTĚ S VOLNOU TOPOLOGIÍ

1.1 BEZDRÁTOVÉ AD HOC SÍTĚ

Bezdrátová Ad hoc síť (obrázek 1.1) je počítačová síť ve které spojovací linky jsou bezdrátové. Síť je Ad hoc protože každý uzel je ochotný předávat data dalším uzlům. To je rozdíl oproti drátovým síťovým technologiím, ve kterých je určený uzel, obvykle s uživatelským hardwarem, známý jako např. router, switch, hub, firewall a vykonává předávání dat. U bezdrátových sítí je tento zvláštní uzel známý jako přístupový bod (AP – *access point*).



Obrázek 1.1 Bezdrátová Ad hoc síť

Minimální konfigurace a rychlé rozmístění dělá Ad hoc sítě vhodné pro nouzové situace jako živelné pohromy nebo armádní konflikty. Decentralizovaná povaha bezdrátových Ad hoc sítí je dělá vhodné pro různé aplikace, kde se nemůžeme spolehnout na centrální uzly, a může zlepšit rozšiřitelnost bezdrátových Ad hoc sítí, ačkoli existují teoretické a praktické omezení celkové kapacity takových sítí.

Ad hoc počítačová síť
Vlastnosti:

- Postrádá pevnou infrastrukturu,
- dynamická povaha sítě (časté změny topologie),
- každý uzel zastává funkci směrovače (routeru),
- obtížná hierarchizace,
- obtížná i minimální centralizace.

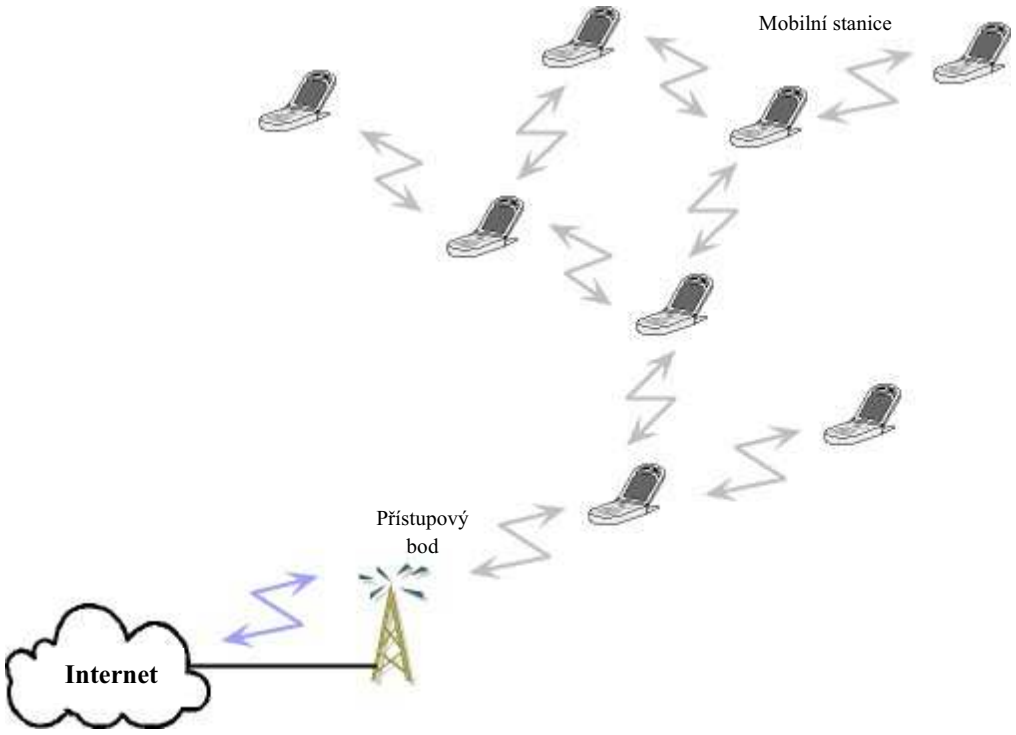
Povaha Ad hoc sítí

- **Sdílení přenosového média** – z čehož vyplývá náchylnost sítě k rušení, omezené sdílené přenosové pásmo a nutnost minimalizace provozu nutného ke správnému směrování.
- **Omezené prostředky mobilních zařízení** – jako výkon, velikost paměti atd.
- **Spotřeba energie**.
- **Dynamická povaha Ad hoc sítí** – časté změny v jejich topologii. Stav sítě se rychle mění, což způsobuje, že uzel má nepřesnou znalost o aktuálním stavu sítě.

Druhy bezdrátových Ad hoc sítí zahrnují mobilní Ad hoc sítě (MANET) a bezdrátové senzorové sítě.

1.1.1 MOBILNÍ AD HOC SÍTĚ (MANET)

Mobilní Ad-hoc sítě MANET (obrázek 1.2) jsou druhem bezdrátových Ad hoc sítí a jedná se o samo-formovací sítě, kdy jsou mobilní směrovače spojeny bezdrátovým spojením, a spojení může tvořit libovolnou topologii. Směrovače se volně náhodně pohybují a sami-organizují tak, že se bezdrátová topologie může měnit rychle a nepředvídatelně. Taková sít může operovat samostatně, nebo může být připojena do internetu.



Obrázek 1.2 Mobilní Ad hoc síť (MANET) s připojením do pevné sítě

Technologie MANET (*RFC 2501*[1]) je synonymem pro mobilní paketové rádiové sítě (*Mobile Packet Radio Networking*), mobilní mesh sítě (*Mobile Mesh Netvorking*) a mobilní, *multi-hop* bezdrátové sítě.

[1] *RFC 2501 dostupné na http://www.ietf.org/rfc/rfc2501.txt.*

Charakteristika MANET

MANET je založena na mobilní platformě (např. router či jiné bezdrátové komunikační zařízení), zde jednoduše označujeme jako uzel, který se volně libovolně pohybuje. Uzly mohou být umístěny na letadlech, lodích, nákladním autě případně i na lidech anebo velmi malých zařízeních. MANET je autonomní systém mobilních uzlů. Systém může operovat samostatně, nebo může mít brány a rozhraní s fixní sítí.

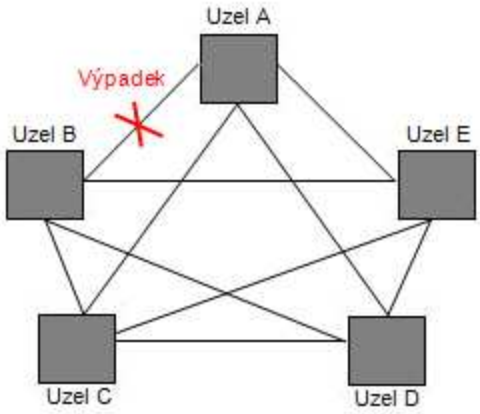
MANET uzly jsou vybaveny bezdrátovými vysílači a přijímači s anténami, které mohou být všesměrové (*broadcast*), směrové (*point-to-point*), nebo kombinované. V daném čase, v závislosti na pozici uzlu, jeho vysílači, pokrytí přijímače, přenosovém výkonu, kanálovým interferencím může mít bezdrátová konektivita mezi uzly formu náhodné, *multi-hop* nebo Ad hoc sítě. Ad hoc topologie se může měnit v čase, jak se uzly pohybují nebo přizpůsobit jejich přenos a parametry přijmu.

MANET má několik hlavních charakteristických rysů:

- **Dynamická topologie** – uzly se libovolně pohybují a tak se topologie sítě může změnit náhodně a rychle v nepředvídatelný čas a mohou se skládat z obousměrných a jednosměrných spojení.
- **Omezená šířka pásma a proměnná kapacita spojů** – bezdrátové spoje budou stále mít významně nižší kapacitu než jejich drátový protějšci. Dále výkon bezdrátové komunikace po uvážení efektu vícenásobného přístupu, úniků, šumu a interferencí je často mnohem menší než maximální přenosová rychlost. Relativně nízká kapacita spojů je typicky způsobena jejích zahlcením např. nashromážděný požadavek aplikace bude pravděpodobně převyšovat kapacitu sítě.
- **Spotřeba energie** – většina uzlů v MANET ke své funkci potřebuje baterie, a proto pro tyto uzly může být nejdůležitějším kritériem návrhu úspora energie.
- **Omezená fyzická bezpečnost** – mobilní bezdrátové sítě jsou obecně náchylnější k bezpečnostním hrozbám než pevné kabelové sítě. Existující bezpečnostní spojovací techniky jsou často aplikovány uvnitř bezdrátových sítí, aby redukovaly bezpečnostní hrozby.

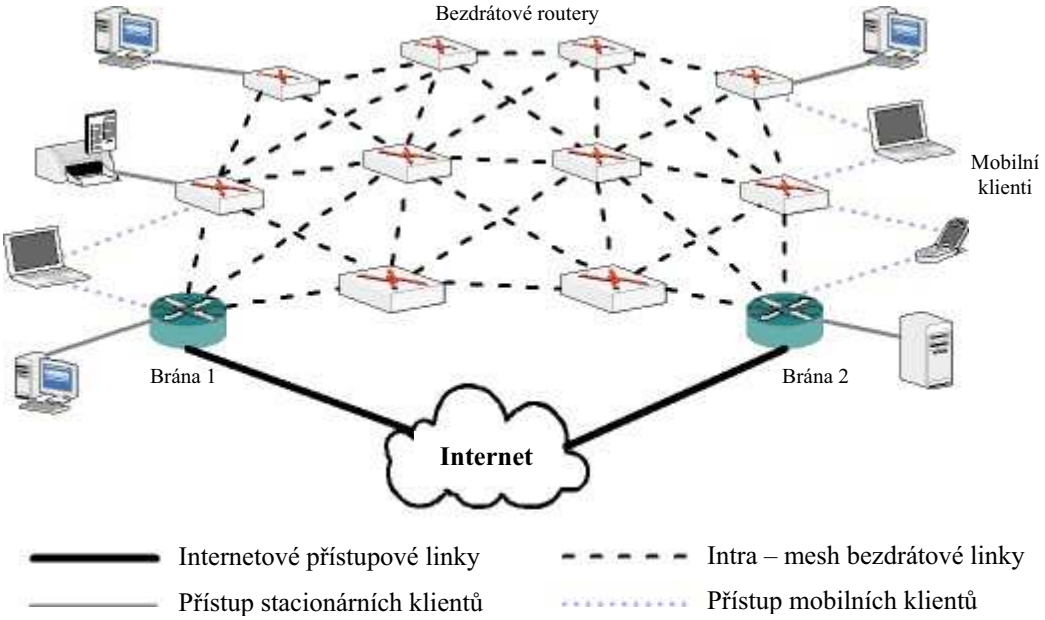
1.1.2 BEZDRÁTOVÉ MESH SÍTĚ

Topologie sítě se smyčkami (*mesh*) nabízí více možných spojů mezi uzly (obrázek 1.3). Může se jednat o plně propojenou síť (*full mesh*), kdy všechny uzly jsou propojeny každý s každým, nebo o částečně propojenou síť (*partial mesh*), kdy se v síti používá méně spojů (uzly, které nejsou propojeny přímo s ostatními, používají ke komunikaci více skoků přes ostatní uzly v síti). Uzly jsou rovnocenné [1].



Obrázek 1.3 Topologie full mesh

Výhodou sítě s touto topologií je vysoká spolehlivost, kdy např. při výpadku spojení mezi uzly A a B existuje možnost alternativní komunikace např. přes uzel E. V důsledku toho vznikají velmi spolehlivé sítě. Nevýhodou je, z důvodu velkého počtu spojů mezi uzly, nákladnost sítě. Obrázek 1.4 ukazuje bezdrátovou mesh síť v praxi.



Obrázek 1.4 Mesh síť

Klient + router = uzel (node)

Hlavní výhodou bezdrátových mesh sítí je schopnost vytvořit síť ihned po zapnutí. Uzly ihned po jejich zapnutí „uslyší“ navzájem svoje vysílání a síť se sama zformuje. Konektivita sítě je automaticky zachovávána. V průběhu několika let procházely bezdrátové mesh sítě vývojem a jsou známy tři generace těchto sítí, z nichž každá přinesla určité zlepšení (rozšiřitelnosti, výkonnosti atd.).

První generace

Tato konfigurace používá jeden rádiový kanál pro služby klientů a pro přepravu zpět *(backhaul*). Jeden rádiový kanál poskytuje obě tyto služby. Z pohledu výkonu nabízí tato architektura nejhorší výsledky, protože obě služby soutěží o kanál resp. jeho šířku pásma. Protože architektura používá pouze jeden kanál, uzel sítě musí nejprve poslouchat, poté posílá data a poté opět poslouchá. Toto chování nepříznivě ovlivňuje výkonnost sítě, zvláště pokud je cíl daleko.

Druhá generace

Každý uzel obsahuje dva rádiové kanály, kdy jeden z nich poskytuje služby klientům a druhý vytváří přepravu zpátečním směrem (*backhaul*). Tyto kanály jsou od sebe oddělené, na sobě nezávislé. Kanály mohou fungovat na různých schématech. Například kanál poskytující služby klientům může využívat 2,4 GHz (802.11 b/g) a kanál pro zpětný přenos 5 GHz (802.11a). Pakety pohybující se směrem k internetu sdílejí šířku pásma v každém „skoku“ podél zpětné cesty s ostatními uzly, které využívají stejný kanál. Toto vede ke snižování výkonnosti sítě. Tato konfigurace je vhodná pro sítě, kde jsou uzly od sebe vzdáleny jeden nebo dva skoky.

Třetí generace

Využívá dva zpětné kanály, jeden pro uplink a druhý pro downlink. Poskytuje separátní přepravu zpětným směrem a službu klientům. Dynamicky řídí všechny kanály tak, aby neinterferovaly. Tato architektura poskytuje nejlepší výkon.

1.1.3 AD HOC VS. MESH SÍTĚ

Hlavní rozdíl mezi bezdrátovými mesh sítěmi a Ad hoc sítěmi je způsob provozu; v mesh síti je provoz buď k bráně, anebo z ní, zatímco v Ad hoc síti je provoz mezi libovolnými páry uzlů. Mohou být užívány i bezdrátové routery, které zlepšují pokrytí a výkonnost sítě. Jsou podobné klientským uzlům, ale nikdy nejsou zdrojem, nebo cílem provozu.

Tabulka 1.1 Srovnání Ad hoc a mesh sítí

Ad hoc síť	Mesh síť
• Uzly jsou bezdrátové, mohou být i mobilní, • může se spoléhat na infrastrukturu, • většina provozu probíhá mezi uživateli.	• Uzly jsou bezdrátové, mohou být mobilní i fixní, • spoléhá se na infrastrukturu, • většina provozu probíhá mezi uživatelem a bránou.

2. MOTOROLA MESH SÍTĚ

Snem velké řady firem, státních institucí, bezpečnostních složek, magistrátů apod., je poskytnout svým zaměstnancům vysokorychlostní přenos dat v podstatě kdekoliv. Zajímavou koncepci v této oblasti představila americká firma Motorola. Nabízí řešení, kde každá koncová stanice současně funguje jako základnová stanice (*access point*). Koncept založený na Motorola MESH architektuře je označován jako MEA – Motorola Enabled Access.

2.1 HISTORIE

Peer-to-peer Ad hoc sítě byly původně vytvořeny pro U.S ozbrojené síly. *The Defense Advanced Research Projects Agency* (DARPA) vydala návrh na vytvoření bezdrátové Ad hoc sítě s následujícími parametry:

- Širokopásmová rychlost přenosu dat,
- koncová podpora IP,
- podpora hlasu a videa,
- určování polohy (bez GPS),
- podpora pro rychlost až do 400 km/hod.

Návrh vytváří robustní, bezpečnou, širokopásmovou síť, která bude okamžitě vytvořena na bojišti, kde není k dispozici dostupná infrastruktura. K tomu, aby se tak stalo, musí být každé klientské zařízení jakousi „bezdrátovou základnovou stanicí“. Několik prominentních obranných dodavatelů vyvinulo systém, který se pokoušel splnit nějaké z požadavků. ITT Industries vyvinul fungující prototypy, které splňovaly všechny požadavky.

Na začátku roku 2000 udělila ITT generální licenci ke komerčnímu využití této technologie firmě Motorola, která navrhla a implementovala tuto technologii do *MN2064A Digital ASIC* a *MEA/QDMA Mobile Broadband Networking Products*. Motorola kompletně integrovala tuto technologii do svého portfolia veřejné bezpečnosti.

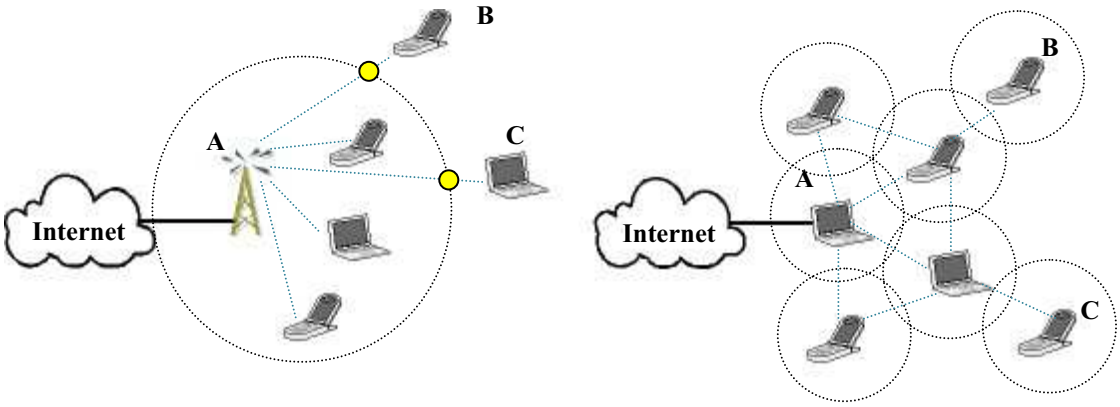
Motorola Enable Access (MEA) technologie se rozvinula v jednu z největší mobilních Ad hoc sítí na světě.

2.2 VLASTNOSTI MOTOROLA MESH SÍTÍ

Jsou to decentralizované, levné, širokopásmové sítě, ve kterých uzel přenáší data pouze k dalšímu uzlu. Uzly působí jako router/repeater k tomu, aby přenášely data z blízkých uzlů uzlům, které jsou daleko (*Motorola Multi – Hopping*). Výsledkem jsou sítě, které mohou překlenout velké vzdálenosti a poskytující vysoké rychlosti přenosu dat. Sítě jsou také extrémně spolehlivé, každý uzel je propojen k několika dalším uzlům. Jestliže nějaký uzel vypadne kvůli poruše, nebo z nějakého jiného důvodu, jeho sousedé si okamžitě najdou jinou cestu. Větší kapacita může být docílena jednoduše přidáním více AP.

Princip je podobný způsobu, jak „cestují“ pakety v internetu. Data přeskakují z jednoho zařízení na další, dokud nedorazí do cíle. To dovoluje implementaci dynamických směrovacích schopností v každém bezdrátovém zařízení. Pro realizaci takové dynamické směrovací schopnosti je potřeba, aby každé zařízení obsahovalo sofistikovaný hardware a software, který může sdělovat směrující informace každému zařízení, které se spojí v reálném čase. Každé zařízení poté určuje co dělat s daty, která přijalo, buď projdou k dalšímu zařízení, nebo budou pozdržena.

Je důležité si uvědomit, že mesh síť není novým typem rádiové modulace, je to pouze nový způsob spojení nynějších a nových rádiových technologií. Mesh síť je spíše užívána jako síťová architektura, než-li zvláštní rádiová technologie. Rádiová modulace určuje, jak se budou přenášet a přijímat informace přes medium (vzduch), zatímco síťová architektura definuje celkovou strukturu, součásti a vzájemné vztahy zařízení v síti. V podstatě to znamená, že MESH technologie mohou být aplikovány na každé z rádiových schémat.

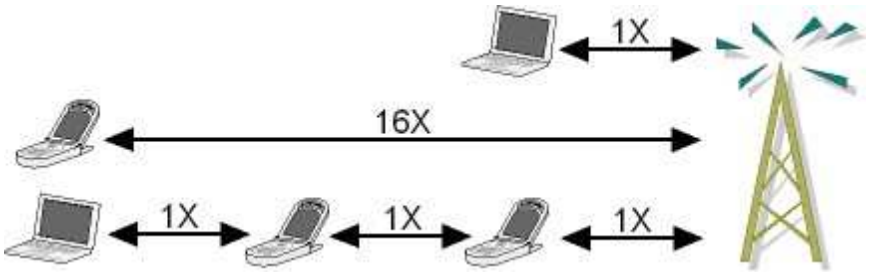


a) *b)*

Obrázek 2.1 a) Tradiční bezdrátová síť, b) Mesh síť

Na obrázku 2.1a je tradiční bezdrátová síť, kde centrálním prvkem je AP (*access point*). Z obrázku je zřejmé, že uzly B a C jsou mimo dosah AP a nemohou se tedy účastnit komunikace. Obrázek 2.1b ukazuje mesh síť, kde každý uzel je router/repeater. Uzly B a C se již mohou účastnit komunikace, a sice „skokem“ přes uzel A.

Širokopásmová bezdrátová komunikace stanovuje kompromis mezi rychlostí přenosu dat a rozsahem pro daný výstupní výkon vysílače. Tj. specifikovaný přenášený výkon, dostupná rychlost přenosu dat (výkonnost) se sníží, jak se zvyšuje vzdálenost od vysílače. Toto platí pro každou radiovou modulaci nebo protokol.



Obrázek 2.2 Vzdálenost k uživateli vs. síla signálu

Na obrázku 2.2 je ukázáno, že pro danou rychlost přenosu dat je požadovaná síla signálu k tomu, aby mohla být poslána data od vysílače k přijímači přes vzdálenost jedné jednotky, je 1×. Ovšem k poslání dat stejnou přenosovou rychlostí k uživateli, který je 3× dál, nepostačí trojnásobek síly, nýbrž 16ti násobek. Mesh mění tuto rovnici rozbitím dlouhé vzdálenosti do několika krátkých vzdáleností (skoků). Výsledkem je, že použitím mesh architektury můžeme poslat stejnou přenosovou rychlostí na stejnou vzdálenost, ale pouze trojnásobkem síly, nikoli 16ti násobkem. Další skutečností je, že v mesh síti je po uzlu požadován přenos pouze 1×, bez ohledu na celkovou vzdálenost přenosu. Tím dochází k prodloužení výdrže baterie a možnosti použití levných radiových součástí.

Přenášený výkon je typicky omezený dostupnou silou baterie na koncovém zařízení. To je důvod proč centralizované (buňkové) sítě nabízejí vysoké rychlosti přenosu dat blízko u buňky nebo AP, ale mnohem nižší rychlosti při pohybu na větší vzdálenosti od nich. To také vysvětluje, proč jsou rychlosti pro downlink (od buňky k mobilnímu uživateli) mnohem vyšší než pro uplink (od mobilního uživatele k buňce) v buňkových systémech.

Mesh nabízí oboje, velký rozsah a vysoké rychlosti přenosu dat skoky přes sérii mezilehlých uzlů. Vzdálenosti mezi uzly (skoky) jsou relativně krátké ve srovnání se vzdáleností mezi koncovým vysílačem a přijímačem. Každý skok může být proveden s mnohem vyšší rychlostí přenosu dat, než je to možné při přímém koncovém spojení. Skoky vytvářejí koncové spojení, které podporuje vysoké rychlosti pro downlink i uplink na velké vzdálenosti.

Systém MEA využívá volné pásmo 2,4 GHz, ale není jím omezen. V mnoha částech světa již funguje ve spektru 4,9 GHz. Prakticky je schopen využívat spektrum od 900 MHz až po zhruba 7 GHz.

Klientská zařízení mají v současné době podobu PCMCIA karet. Motorola ale pracuje i na jiných podobách.

2.3 VÝHODY MOTOROLA MESH SÍTÍ

Okamžité a automatické formování bezdrátové sítě

Vrcholem technologie mesh je schopnost uzlu se automaticky kdykoliv připojit do sítě, nebo odpojit ze sítě. Signály jsou optimálně směrovány, jak síť roste a vyvíjí se. Síť může být sestavena prakticky okamžitě a kdekoliv, dokonce i v místech s infrastrukturou. Ve skutečnosti i zařízení pohybující se rychlostí až 240 km/hod se mohou automaticky připojit do mesh sítě, což umožňuje úplně nové modely mobility.

Samo-formovací, samo-regenerační a samo-vyrovnávací technika

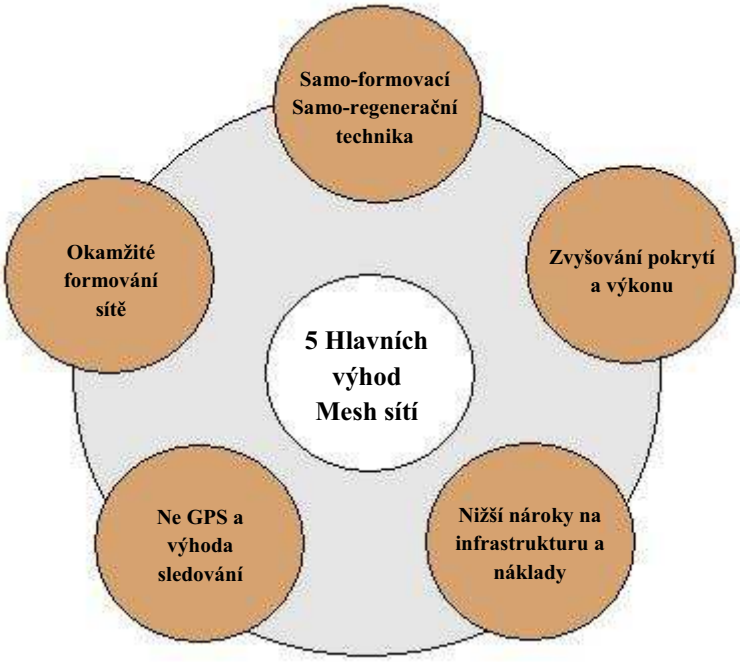
Mesh sítě jsou více robustní než-li tradiční bezdrátové sítě. Automatická konfigurace a směrování umožňuje síti být samo-formovací a samo-regenerační. Síť funguje i po selhání jednoho nebo několika uzlů. Mohou být spolehlivě sestaveny téměř okamžitě, bez přítomnosti infrastruktury.

Zvyšuje pokrytí a výkon

Vysoká datová propustnost vyžaduje velký odstup signálu od šumu. Nicméně signál slábne exponenciálně, jak se vzdálenost od vysílače zvětšuje, což znamená vyšší šum a nižší výkon. Ovšem v mesh sítích každý uzel vystupuje jako router/repeater tzn., obnovuje intenzitu signálu s každým „skokem“ v síti. To má za následek, že síť může mít prakticky jakoukoliv velikost při zachování výborného výkonu.

Nižší nároky na infrastrukturu a nižší provozní náklady

Mesh sítě typicky požadují menší přepravu zpátečním směrem, než tradiční bezdrátové sítě, někdy až o 90%, což velmi redukuje provozní náklady. Vzhledem k tomu, že se jedná o samo-formovací a samo-regenerační sítě jsou i administrační náklady a náklady na údržbu rovněž nižší. Dovednosti administrátora mohou být nižší, než je typicky požadované pro celulární a další centralizované bezdrátové sítě. Sítě jsou rovněž „samo-hojivé“ (což znamená, že při výpadku některého z uzlů dovedou najít alternativní cestu k cíli), čímž je velmi snížena potřeba 24 hodinové podpory.



Obrázek 2.3 Výhody Motorola Mesh sítí

Ne-GPS a výhoda sledování

GPS je výhoda pro organizace, které potřebují způsob, jak lokalizovat lidi a věci v pohybu. GPS ale také podléhá několika nedostatkům a sice, nefunguje např. v dolech, uvnitř rozsáhlých struktur nebo v místech, která blokují signál z GPS družic. Motorola MESH technologie používá důmyslný triangulační[2] algoritmus k tomu, aby určil umístění uzlů, a uživatelů v síti tzn. například schopnost nalézt požárníka v hořící budově, nebo v místech kde není dostupný GPS signál.

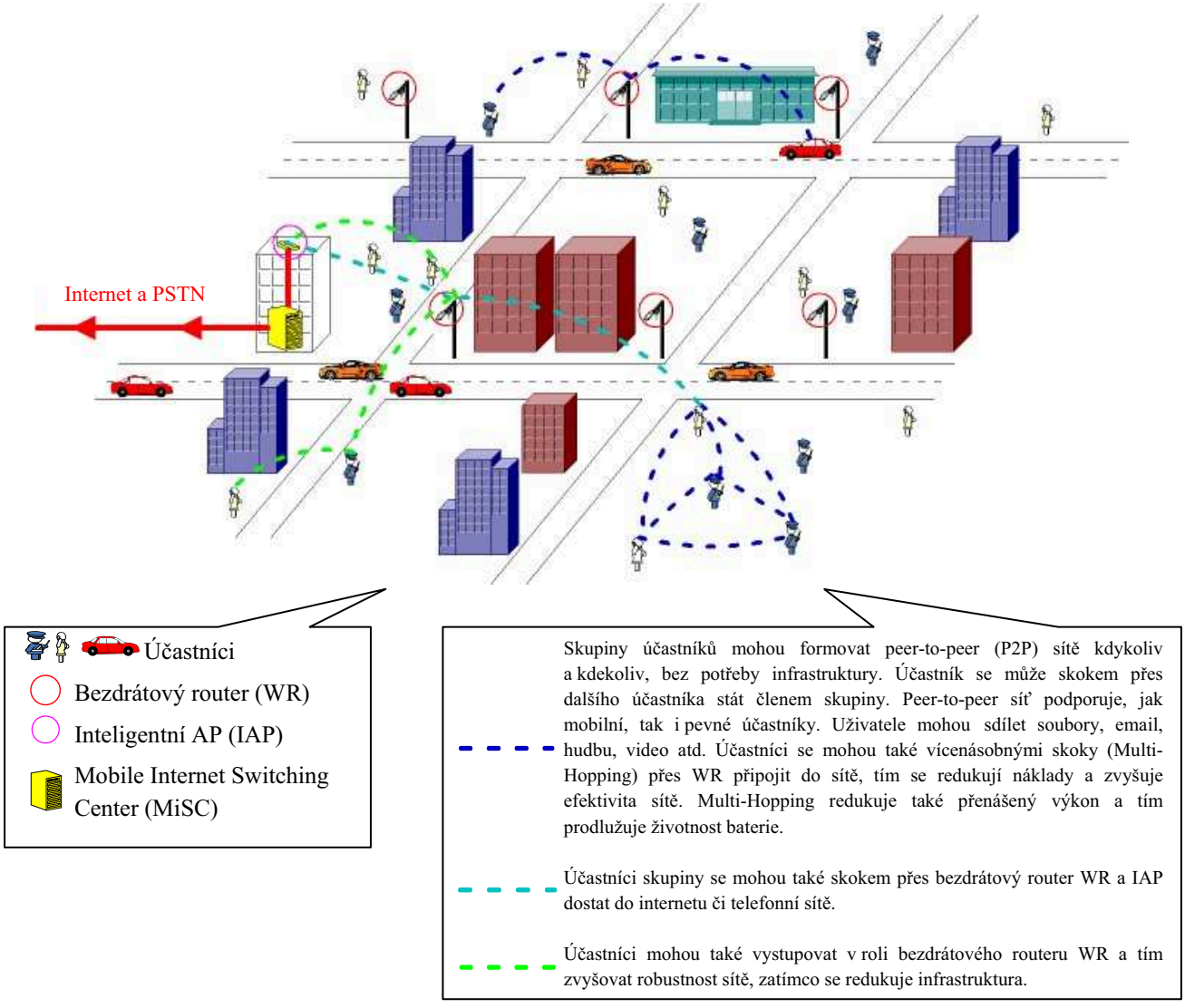
[2] *Triangulace – metoda určování polohy a vzdálenosti.*

2.4 MOTOROLA MESH SÍTĚ V PRAXI

Motorola nabízí kompletní škálu jak hardwarových součástí, tak i softwarových aplikací pro rychlé rozestavení širokopásmových mobilních sítí, nabízejících vysoký výkon. Tyto produkty je možné využít v mnoha aplikacích, včetně veřejné bezpečnosti, dopravy a městských širokopásmových sítí.

Tato mobilní širokopásmová síť kombinuje škálovatelnou, výkonnou a patentovanou mobilní Ad hoc síť patřící do MEA technologie s výkonným QDMA přístupem. Výsledkem je cenově přístupné, schopné, samo-formovací a samo-regenerační bezdrátové řešení pro komunikaci.

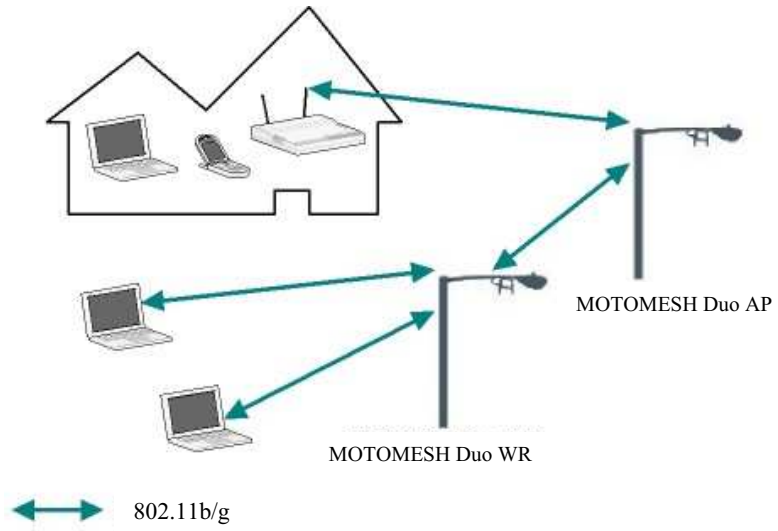
2.4.1 MOTOMESH SOLO



Obrázek 2.4 MOTOMESH Solo

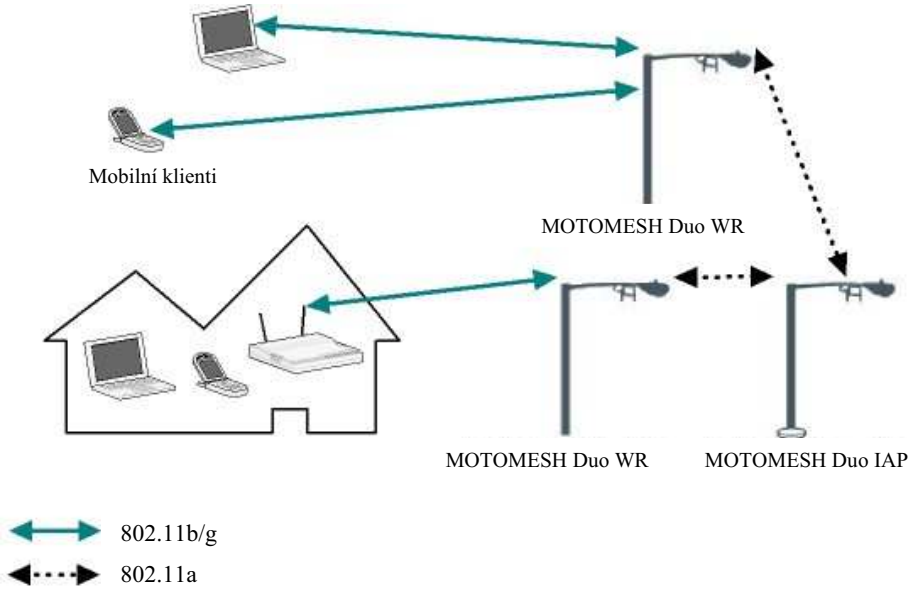
2.4.2 MOTOMESH DUO – DALŠÍ GENERACE WIFI MESH ŘEŠENÍ

MOTOMESH Duo je dostupné buď v jediné rádiové konfiguraci (obrázek 2.5), využívající přenosové pásmo 2,4 GHz (WiFi 802.11b/g) nebo ve dvojí konfiguraci (obrázek 2.6) s dodatečným přenosovým pásmem 5,8; 5,4 nebo 4,9 GHz (802.11a). V první konfiguraci je pásmo 2,4 GHz použito jak pro klientský přístup, tak i pro přístup mezi uzly mesh. Volba tohoto typu konfigurace je ideální pro řešení, kde je hlavním faktorem pokrytí a nízká cena.



Obrázek 2.5 MOTOMESH Duo 802.11 b/g

V konfiguraci druhé je pásmo 5,8; 5,4 nebo 4,9 GHz vyhrazeno pro provoz mezi mesh uzly, zatímco pásmo 2,4 GHz pro klientský přístup. Tato konfigurace oproti první podává zvýšený výkon, mírnější interference a nižší zpoždění.

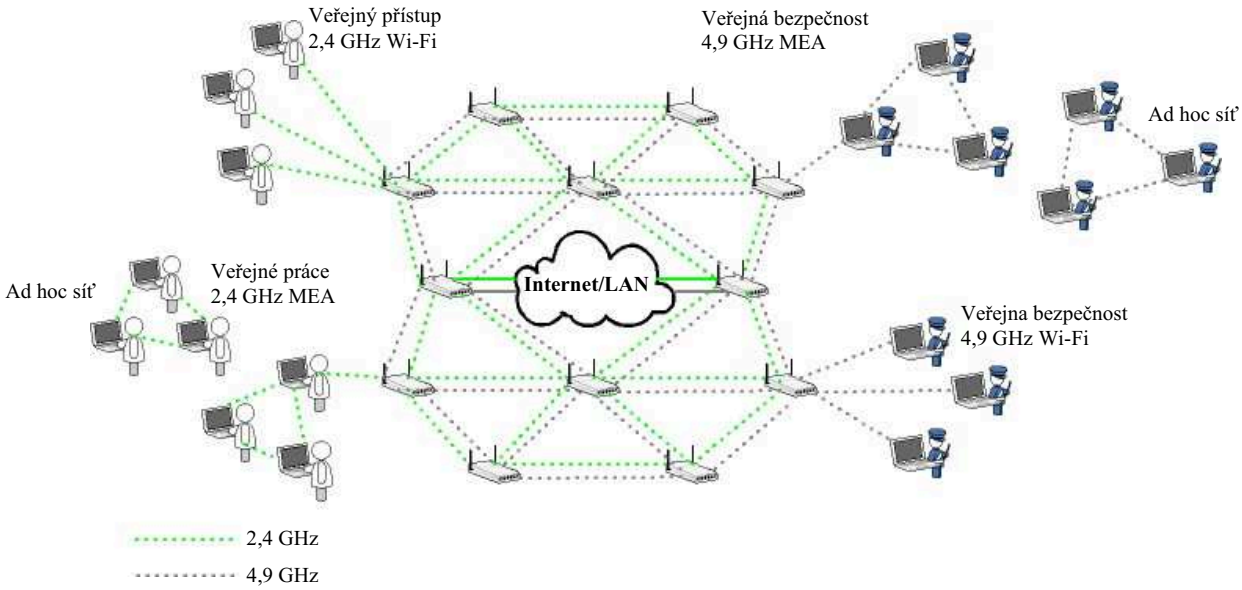


Obrázek 2.6 MOTOMESH Duo 802.11b/g a 802.11a

2.4.3 MOTOMESH QUATTRO

MOTOMESH Quattro (obrázek 2.7) je široké multi-rádiové řešení, které nabízí bezpečnost, kapacitu a flexibilitu potřebnou zejména ve větších městech. Může poskytovat mobilní širokopásmový přístup pro různorodé městské instituce, stejně jako WiFi přístup pro veřejnost. Architektura Quattro podporuje až čtyři pásma sítí v jednom přístupovém bodu a je postavena na MEA technologii. Dále podporuje vysokorychlostní data, video a službu určení polohy pro pevné a mobilní uživatele.

Využívá licencované pásmo 4,9 GHz a nelicencované pásmo 2,4 GHz. Každý MOTOMESH přístupový bod obsahuje dva standardy vyhovující 802.11 (WiFi) a dva vyhovující MEA (*Motorola Enable Access*). Jedna sada WiFi a MEA pracuje v nelicencovaném pásmu 2,4 GHz a ostatní v pásmu veřejné bezpečnosti 4,9 GHz. Každé MEA pásmo vystupuje jako router/repeater pro všechny další MEA zařízení v síti. Uživatelé mohou skokem přes sousední zařízení komunikovat mezi sebou, nebo komunikovat se vzdáleným přístupovým bodem, který je může spojit s dalšími sítěmi.



Obrázek 2.7 MOTOMESH Quattro

2.4.4 SPECIFIKACE KOMPONENT MOTOROLA MESH SÍTĚ

MOTOMESH uzly mohou být nainstalovány na široké množství míst, včetně světelných a užitkových tyčí, dopravních návěstí, budov atd. Jedna osoba může nainstalovat mesh modul během 15 minut, modul se automaticky zapne a začlení do systému, přičemž osoba nemusí být odborně školena.

Bezdrátový modem (WMC6300)

Bezdrátový modem (obrázek 2.8) nabízí rychlost přenosu dat až 6 Mbps pro audio i video, rychlé a přesné určení pozice a řadu dalších služeb pro zařízení s PCMCIA slotem. Bezdrátový modem může také vystupovat jako router, tím se zvyšuje robustnost sítě a rozsah, ale nezvyšují se náklady.

Obrázek 2.8 Bezdrátový modem

Tabulka 2.1 Parametry bezdrátového modemu

Parametry modemu	
Modulace	QDMA
Kmitočet [GHz]	2,4-2,4835
Max. přenosová rychlost	6 Mbps
Výstupní výkon	23 dBm
Rozhraní	PCMCIA
Spotřeba (Vysílání)	3,3 W
Spotřeba (Přijímání)	1,5 W

Bezdrátový router (MWR6300)

Bezdrátový router (obrázek 2.9) je malé, levné bezdrátové zařízení, které poskytuje garantované pokrytí na velké zeměpisné oblasti, školní areály, nebo může být použito i uvnitř budov. Dále jsou používány pro rozmístění nových sítí a umožňují bezdrátovou komunikaci mezi klientem IAP.

Obrázek 2.9 Bezdrátový router

Tabulka 2.2 Parametry bezdrátového routeru

Parametry routeru	
Modulace	QDMA
Kmitočet [GHz]	2,4-2,4835
Max. přenosová rychlost	6 Mbps
Výstupní výkon	až 25 dBm

Inteligentní AP (IAP6300)

Inteligentní AP (obrázek 2.10) je rovněž malé a levné zařízení, které tvoří jakýsi přechod z bezdrátové MEA sítě do internetu nebo PSTN. Každý IAP podporuje rychlost přenosu dat až 6 Mbps. Kdykoliv můžeme zvýšit kapacitu sítě rozmístěním dalších IAP.

Obrázek 2.10 Inteligentní AP

Tabulka 2.3 Parametry IAP

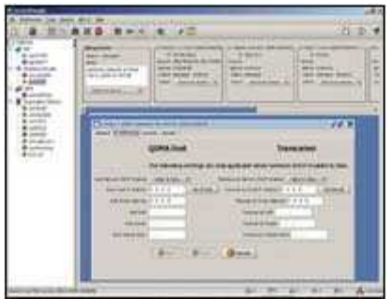
Parametry IAP	
Modulace	QDMA
Kmitočet [GHz]	2,4-2,4835
Max. přenosová rychlost	6 Mbps
Výstupní výkon	až 25 dBm
Síťové rozhraní	10/100 Mbps Ethernet (RJ-45)

Mobile Internet Switching Center (MiSC)

MiSC poskytuje směrovací, přepojovací a řídící funkce pro MEA síť. Zajišťuje konektivitu mezi IAP a „drátovým" světem. Administrátor může monitorovat a řídit celou síť prostřednictvím tzv. MeshManageru, což je program, který poskytuje celou řadu nástrojů pro správu klientů a síťové infrastruktury.

MeshManager EMS – Element Management System

EMS (obrázek 2.11) poskytuje kompletní řešení pro konfiguraci, chybové stavy, výkon a bezpečnost v Motorola MESH síti. Obsahuje grafické uživatelské rozhraní založené na Java™ a serii softwarových serverů. MeshManager umožňuje pomocí několika kliknutí přístup k potřebným nástrojům pro kompletní konfiguraci a kontrolu nad sítí.



Obrázek 2.11 MeshManager EMS

Tabulka 2.4 Parametry EMS

Parametry EMS	
Podporované OS	Windows XP Windows Server 2003 RedHat Linux v3.0
Podporované MOTOMESH sítě	MEA 2,4 GHz MOTOMESH 2,4 GHz, 4,9 GHz Mesh Camera Wireless Video Systém

3. QoS (Quality of Services)

Internet byl původně vybudován s cílem poskytnout službu „dobré vůle“, tedy bez zajištění doručení datagramů do určité doby. Starší síťové technologie poskytovaly všem datovým jednotkám stejný způsob zacházení („best effort“). Na první pohled se tento způsob zacházení zdá být spravedlivý, ale není tomu tak, protože neposkytuje žádné garance. V rámci této úrovně však neexistuje jistota, že potřebná úroveň přenosové služby bude zajištěna po celou dobu relace.

Zpoždění či ztráty jsou v rámci best effort nepředvídatelné, a tedy nijak nezajištěné v rámci určitých mantinelů [1]. Datové toky odpovídající určitým službám jsou různě citlivé na zpoždění, kolísání zpoždění, ztráty paketů atd. Citlivost jednotlivých aplikací na tyto veličiny ukazuje tabulka 3.1 a konkrétní hodnoty parametrů QoS uvádí tabulka 3.2.

Tabulka 3.1 Citlivost různých typů dat v síti [1]

Typ provozu	Citlivost na			
	Šířku pásma	Ztrátu paketů	Zpoždění	Kolísání
Hlas	velmi nízká	střední	vysoká	vysoká
Elektronický obchod	nízká	vysoká	vysoká	nízká
Transakce	nízká	vysoká	vysoká	nízká
Email	nízká	vysoká	nízká	nízká
Telnet	nízká	vysoká	střední	nízká
Občasné prohlížení webu	nízká	střední	střední	nízká
Náročnější prohlížení webu	střední	vysoká	vysoká	nízká
Přenos souborů	vysoká	střední	nízká	nízká
Videokonference	vysoká	střední	vysoká	vysoká
Skupinové vysílání	vysoká	vysoká	vysoká	vysoká

Tabulka 3.2 Parametry QoS [1]

Typ provozu	Maximální jednosměrná latence	Maximální kolísání (jitter)
Hlas po IP	200 ms	30 ms
Videokonference	200 ms	30 ms
Streaming video	5 s	–

V dnešních sítích se používají dva hlavní způsoby zajištění QoS a sice IntServ *(Integrated Services)* a DiffServ *(Differentiated Services)*.

3.1 INTSERV (INTEGRATED SERVICES)

Technologie integrovaných služeb *(Integrated Services – IntServ)* je schopna rozlišit každý datový tok na základě identifikátorů (např. síťová adresa, identifikátor uživatelské aplikace) odesílatele a příjemce. Proto je schopna zajistit řízení kvality služeb po celé trase od zdroje až k cílové stanici [4].

Používá se ve spojitosti s protokolem *RSVP (Resource ReSerVation Protocol).* Vyžaduje spoluúčast všech směrovačů, které musí udržovat informace o stavu každého toku dat. Jak roste počet toků dat, roste tím logicky i objem těchto informací, které musí směrovače uchovávat a zpracovávat. Což je nevýhoda tohoto modelu, protože se tím zvyšují paměťové a výkonnostní nároky na směrovače.

Uplatnění IntServ je např. v podnikových sítích.

Pro správnou funkci IntServ musí být ve směrovačích a hostitelích (odesílatel a příjemce QoS) implementovány následující komponenty:

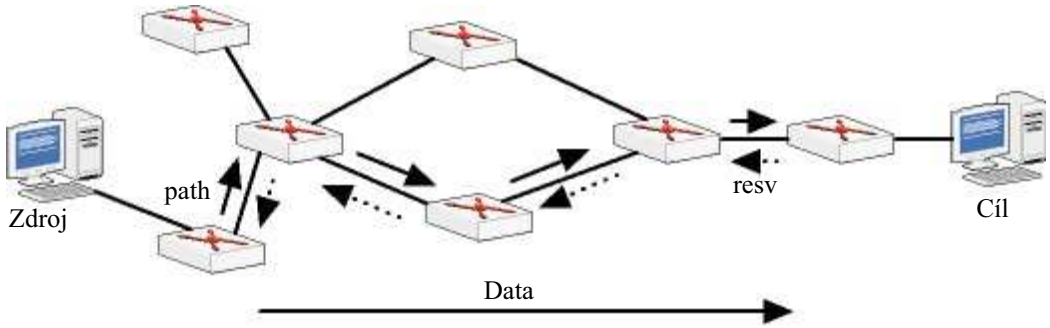
- **Plánovač paketů** – řídí zasílání různých proudů paketů, použitím front, časovačů a dalších mechanizmů. Je implementován v místě, kde se pakety řadí do front.
- **Kontrola přístupu** – provádí rozhodovací algoritmus, který určuje, zda-li novému toku může být udělena rezervace.
- **Klasifikátor.**
- **RSVP Protokol.**

3.1.1 RSVP (RESOURCE RESERVATION PROTOCOL)

Protokol využívá cílová stanice, která očekává určitá data a chce si pro ně zajistit zaručený průchod sítí. Protokol poté signalizací zjišťuje po celé cestě sítí všemi směrovači až ke zdrojové stanici, zda žádaná šířka pásma může být pro daný tok přidělena. Protokol tedy garantuje šířku pásma prostřednictvím vybudované cesty mezi koncovými uzly s dohodnutými parametry ve specifikaci toku, v každém směrovači nebo přepínači.

Pro komunikaci mezi uzly se používají dva druhy zpráv, jejichž využití pro rezervaci prostředků ilustruje obrázek 3.1:

- **Resv** – specifikuje požadavky (od příjemce) na vytvoření, změnu a zrušení rezervace prostředků.
- **Path** – nese informace od odesílatele nebo jiného uzlu sítě o toku dat.



Obrázek 3.1 Rezervace prostředků pomocí RSVP

3.2 DIFFSERV (DIFFERENTIATED SERVICES)

Diferencované služby (*Differentiated Services – DiffServ*) dělí síťový provoz do několika málo tříd a pak zajišťuje odlišné zacházení pro tyto třídy. DiffServ proto není schopen garantovat parametry pro jednotlivé datové toky, ale má výrazně menší nároky na výkonnost aktivního prvku a je výrazně lépe škálovatelný, než technologie IntServ [4].

DiffServ využívá z pole ToS v IP datagramu namísto původních 3 bitů pro IP precedent bitů 6, jako DSCP (*DiffServ Code Point*). DSCP dovoluje třídit síťový provoz do 64 tříd. Provoz vstupující do sítě je klasifikován na hranici sítě a přidělen k seskupení datagramů se stejným chováním, tedy BA (*Behavior Aggregate*), poté se BA zakóduje do DSCP. DSCP analyzuje klasifikátor a provádí pro daný paket úpravu provozu, měření, označování atd.

DiffServ se hodí do jádra sítě, zatímco IntServ na její okraj.

3.3 QoS Optimalizace v MANET

V mobilních Ad hoc sítích přítomnost šířky pásma, spojovacího omezení, stejně jako stálá změna topologie sítě, dělají zajištění QoS v těchto sítích těžší, než-li u sítí založených na drátovém vedení, kde je pouze potřeba zajistit dohodu o šířce pásma nebo paměti [6]. Kvůli nedostatku dostatečně přesných znalostí síťových stavů (okamžitých i předvídaných) mohou být garance QoS nemožné, jestliže jsou uzly vysoce mobilní. Proto mnoho řešení QoS vyvinutých pro internet nejsou vhodná pro MANET, je potřeba, aby byla přizpůsobena.

Obecně QoS nesouvisí s žádnou určenou síťovou vrstvou, ale přesněji vyžaduje podporu všech vrstev [6]. Důležité součásti QoS v MANET doméně zahrnují:

- **QoS model** – naznačuje celkové QoS cíle a architekturu, pro zavedení dané aplikace nebo služby. Tyto cíle mohou obsahovat kapacitu spojení, zpoždění, vytížení, výkonnost, šířku pásma, spotřebu energie atd.
- **QoS směrování (*QoS routing*)** – zajišťuje zjištění a údržbu cesty tak, aby splnila QoS cíle, dané omezením zdroje.
- **QoS signalizace (*QoS signalization*)** – je zodpovědná za kontrolu přijetí a plánování, stejně jako za rezervaci zdrojů podél cesty určené QoS směrováním nebo dalšími protokoly.

QoS model specifikuje architekturu, která nám umožňuje poskytnout službám model, který funguje lépe než model best effort, který existuje v MANET. Tato architektura by měla brát ohled na výzvy MANET sítí, jako je dynamická topologie a v čase se měnící spojovací kapacita. Výše je již popsán základní koncept QoS pro nynější drátové sítě (IntServ/RSVP a DiffServ). Níže budeme analyzovat důvody, proč výše uvedené modely nejsou vhodné pro MANET a představíme první navržený QoS model pro MANET a sice FQMM.

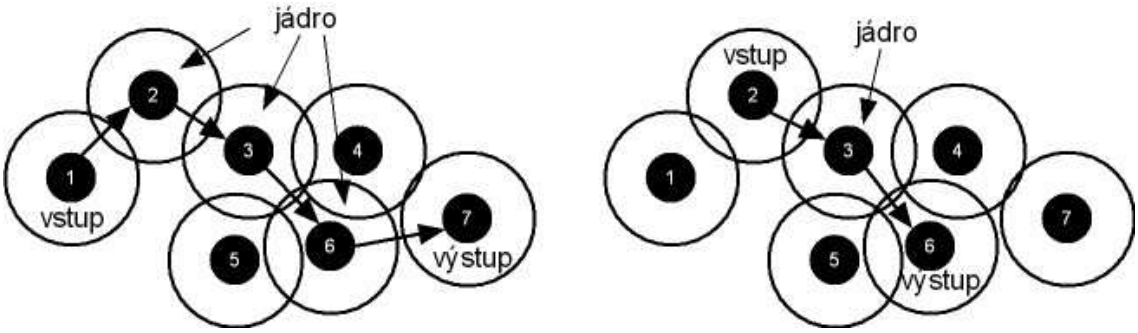
IntServ/RSVP model není vhodný pro MANET kvůli omezeným zdrojům v MANET. Je zde několik faktorů, které nedovolují použití tohoto modelu v MANET:

- Obrovské nároky na paměť a zpracování režijních informací pro každý mobilní uzel, protože si musí udržovat takovou informaci. Navíc množství těchto informací se zvyšuje úměrně s počtem toků, což je také problém nynějšího internetu, ale který byl vyřešen hromaděním těchto informací na *core* routerech (*DiffServ*).
- RSVP rezervace a proces údržby je sítí pohlcující procedura. RSVP signalizační pakety budou soutěžit s datovými pakety o šířku pásma.

DiffServ je na druhé straně povrchní model pro vnitřní routery, protože jednotlivé toky jsou shromažďovány do skupiny toků. Toto dělá směrování v jádru sítě o hodně snadnější. Tento model by tedy mohl být potencionálně vhodný pro použití v MANET. Ovšem v MANET síti neexistuje přesná definice toho, co je jádro (*core*), vstupní nebo výstupní router, protože topologie sítě je dynamická. V úplné Ad hoc topologii, kde není žádný poskytovatel služeb, a kde jsou pouze klienti, je docela obtížné zavádět QoS, protože neexistuje žádný závazek od někoho k někomu, což dělá QoS téměř nemožné.

FQMM (*Flexible QoS Model for MANET*) je první QoS model navržený pro MANET v roce 2000. Představa je spojit znalost z řešení v drátové síti a použít je na nový QoS model, který bude brát ohled na charakteristické rysy MANET. Základní představa tohoto modelu je, že se užívají jak vlastnosti IntServ, tak i diferencování služeb DiffServ. Jinými slovy, tento model navrhuje, že nejvyšší priorita je přiřazena toku a další priority jsou přiřazeny třídám. Dále je tento model založený na předpokladu, že ne všechny pakety v síti ve skutečnosti vyžadují nejvyšší prioritu, protože poté by tento model vedl k podobnému modelu, jako IntServ, kde je poskytována služba všem tokům. FQMM hybridní model definuje tři typy uzlů (obrázek 3.2), přesně jako DiffServ, a sice:

- Vstupní, jestliže posílá data.
- Jádro (*core*), jestliže předává data.
- Výstupní, jestliže přijímá data.



Obrázek 3.2 Uzly v FQMM

Rozdíl je v tom, že uzel v FQMM nemá nic společného s jeho fyzickým umístěním v síti, což by z podstaty MANET nemělo žádný smysl.

4. SMĚROVACÍ PROTOKOLY V SÍTÍCH S VOLNOU TOPOLOGIÍ

Protokoly lze na základě jejich vlastností rozdělit do několika skupin:

- **Proaktivní** (tabulkou řízené) – protokol v tabulce udržuje trvale kompletní směrovací informace o celé síti. Výhodou je znalost cesty v okamžiku její potřeby, z čehož plyne nízké zpoždění. Naopak hrozí zahlcení sítě šířením směrovacích informací. Jsou vhodnější pro sítě s menším počtem uzlů a s nižší četností změn v síti. Tabulka se aktualizuje vždy při změně v síti nebo automaticky v průběhu. Do této skupiny patří např. protokoly DSDV *(Destination Sequenced Distance Vector)* a OLSR *(Optimized Link State Routing).*

- **Reaktivní** – cesta k cíli se hledá až v okamžiku potřeby a uchovány jsou pouze aktivní cesty. Nevýhodou je zpoždění při hledání cesty. Jsou vhodné pro rozlehlé sítě, pro sítě s větším počtem uzlů a pro sítě s častou změnou topologie. Patří sem protokoly AODV (*Ad Hoc On Demand Distance Vector Routing)* a DSR (*Dynamic Source Routing)*.

- **Hybridní** – kombinace proaktivního a reaktivního směrování. Do vzdálenosti přes jednoho souseda se užívá proaktivní směrování a udržuje se kompletní směrovací tabulka. Pro vzdálenější uzly se používá reaktivní směrování. Do této skupiny lze zařadit např. protokol ZRP (*Zone Routing Protocol)*.

- **Geografické** – směrování na základě fyzické polohy zařízení. Předpokladem je znalost polohy uzlu např. pomocí GPS nebo jiného vyhledávacího systému.

- **Hierarchické** – síť je rozdělena do určitých oblastí, jejichž činnost řídí určený uzel, několik různých oblastí zase obsluhuje jiný uzel.

4.1 SMĚROVACÍ PROTOKOLY V MANET

4.1.1 SMĚROVÁNÍ V MANET

Velký růst v oblasti použití mobilních zařízení spolu s uživateli real-time aplikací poskytl nové výzvy v návrhu protokolů pro MANET sítě. Hlavní mezi těmito výzvami, která souvisí s real-time aplikacemi pro MANET je začlenění podpory QoS, jako šířka pásma nebo zpoždění. Zvláště jsou důležité ty směrovací protokoly, které včleňují QoS metriky v nalezení cesty a udržení, aby podporovaly koncové QoS.

MANET sítě se liší od dalších druhů sítí jejich fyzickými charakteristickými rysy, organizačním formátem a dynamickou topologií:

- **Fyzická charakteristika** – bezdrátové kanály jsou náchylné k chybám díky únikům, interferencím a stínění, což způsobuje nepředvídatelnou šířku pásma a zpoždění paketů.
- **Organizační formát** – distribuovaná povaha MANET znamená, že kanálové zdroje nemohou být přiřazeny předem určené cestě.
- **Dynamická topologie** – spojení jsou vytvářena a ničena nepředvídatelně. Stav sítě se mění rychle, což způsobuje, že uzel má nepřesnou znalost o aktuálním stavu sítě.

Z důvodu mobility zařízení v MANET síti a sdílené povahy bezdrátových prostředků je nabídka QoS garancí, jako šířka pásma, zpoždění a kolísání zpoždění nepraktická. Místo toho jsou navrhována QoS adaptace a soft QoS. Soft QoS dovoluje selhání QoS, například když dojde ke ztrátě cesty nebo se síť rozdělí. Jestliže se síť mění příliš rychle, je šíření informací o topologii výzvou, kterou soft QoS nabízí. Kombinatorická stabilita znamená, že je dáno specifické časové okno topologie. Změna topologie se poté děje dostatečně pomalu, aby se mohli úspěšně šířit všechny topologické změny podle potřeby, což je nezbytné k poskytování QoS.

Některé aplikace, jako real-time aplikace mohou optimalizovat svůj výkon podle dostupných síťových zdrojů, což je výhodné pro QoS. Například vrstvové kódování dovoluje vyšším vrstvám poskytnutí různé úrovně kvality. Minimální šířka pásma je garantována základní vrstvou. Poskytnutí odezvy aplikaci o dostupných zdrojích dovoluje aplikaci měnit kódovací strategii, aby poskytla nejlepší kvalitu i pro omezené zdroje.

Směrování je využíváno pro zřízení a udržení cesty mezi uzly podporujícími přenos dat. První MANET směrovací protokoly se zaměřovaly na nalezení vhodné cesty od zdroje k cíli, bez jakéhokoliv zřetele na optimalizaci využití síťových zdrojů nebo podpory specifických požadavků aplikací. Hlavním problémem je nalezení vhodné cesty z dostupných zdrojů, tak aby splňovala QoS omezení spolu s optimalizací, jako nalezení nejlevnější a nejstabilnější cesty. Stanoveny jsou tyto cíle, následně je proveden základní návrh QoS směrovacího protokolu.

- **Zdrojový odhad** – nabízí zdrojovou garantovanou cestu, klíčové je získání informací o dostupných zdrojích z nižších vrstev. Tato informace pomáhá ve vykonávání přístupu a QoS přizpůsobování. Většina existujících technik se soustřeďuje na QoS omezení jako šířka pásma nebo zpoždění, a tak šířka pásma dostupná pro uzel nebo spojovací linku anebo zpoždění musí být odhadována. V MANET uživatelé sdílejí šířku pásma se svými sousedy, a tak šířka pásma dostupná pro uzel se mění a je dynamicky ovlivňována provozem jeho sousedů. Proto mezi dva klíčové problémy pro odhad šířky pásma patří: jak přesně a jak často je odhadována dostupná šířka pásma. Obecně je klíčovou záležitostí kompromis mezi výhodou z užívání zdrojového odhadu, ceny v rámci režií a výpočetní náročností, která je použita pro zdrojový odhad.

- **Nalezení cesty** – existují dva hlavní přístupy ke směrování v MANET, reaktivní a proaktivní směrování. Reaktivní směrování redukuje režijní náklady na úkor zpoždění v nalezení vhodné cesty, zatímco u proaktivního směrování je tomu naopak. Další záležitostí je určení kombinace snížení zpoždění a snížení nákladů, která je nejlepší pro podporu QoS.

- **Rezervace zdrojů** – jak je uvedeno výše, šířka pásma je sdílená se sousedními uživateli v MANET. Proto další náročnou záležitostí je jak přidělit tyto sdílené prostředky, typ schématu pro rezervaci zdrojů a druh přístupu, které by měli být užívány pro nastavení a údržbu QoS cesty.

- **Udržení cesty** – pohyblivost uzlů v MANET sítí způsobuje častou změnu topologie sítě, což způsobuje obtížné plnění QoS omezení. Zařazení udržovacího schématu do QoS směrování je čtvrtý činitel návrhu. Typický přístup k udržení cesty, která způsobuje čekání na objevení poruchy cesty, významně ovlivňuje směrovací výkon. Proto predikční schéma nebo redundantní směrování pomáhá při údržbě cesty.

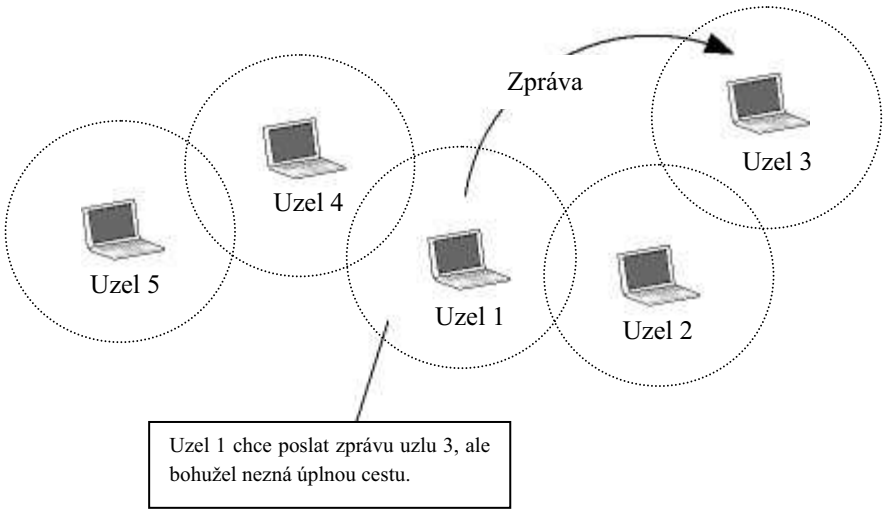
- **Výběr cesty** – QoS směrování má mnoho přísných požadavků na stabilitu cesty, protože častá selhání nepříznivě ovlivňují QoS. Cesta s největší dostupnou šířkou pásma není jedinou uvažovanou, další metrika jako spolehlivost cesty a délka cesty by také měla být brána v úvahu při výběru cesty. Bylo vyvinuto několik směrovacích protokolů podporujících QoS jednou z následujících cest:
  - Výběr cesty s největší dostupnou šířkou pásma (nebo minimálním zpožděním).
  - Odmítnutí cestovní žádosti, jestliže je k dispozici nedostatečná šířka pásma.
  - Poskytnutí aplikaci odezvu o dostupné šířce pásma nebo odhadu zpoždění.

4.1.2 AODV (AD HOC ON DEMAND DISTANCE VECTOR)

Charakteristika AODV:

- Hledá cesty jen v případě potřeby,
- používá pořadová čísla ke sledování přesnosti informací,
- sleduje pouze další skok v cestě, nikoli celou cestu,
- používá periodické posílání *HELLO* zpráv ke sledování sousedů.

AODV je metoda ke směrování zprávy mezi mobilními počítači. Dovoluje tomuto počítači, nebo uzlu poslat zprávu skrz sousední uzly, se kterými nemohou přímo komunikovat. AODV toto dělá hledáním cesty, podél které mohou být zprávy posílány. AODV se ujišťuje, že tyto cesty neobsahují smyčky a zkouší hledat nejkratší možnou cestu. AODV je také schopen reagovat na změny v cestách a může vytvářet nové, jestliže došlo k chybě. Obrázek 4.1 ukazuje schéma tvořené čtyřmi uzly na bezdrátové síti. Kruhy ilustrují rozsah komunikace pro každý uzel. Protože rozsah je limitován, každý uzel může komunikovat pouze s uzly vedle sebe.

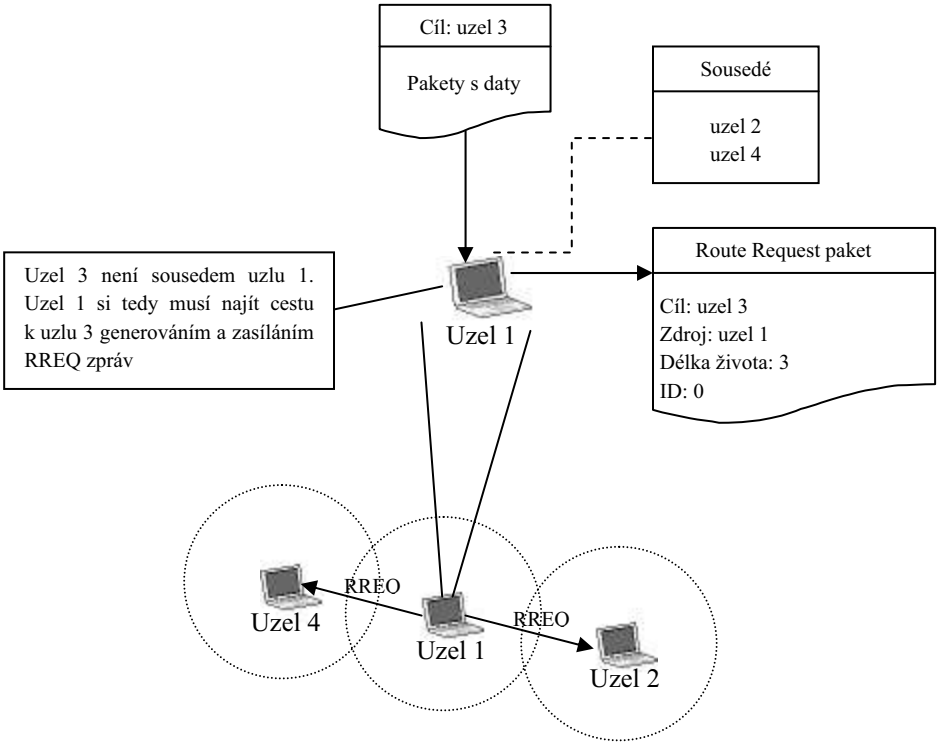


Obrázek 4.1 Ukázka AODV

Uzly, se kterými lze komunikovat přímo jsou považovány za sousedy (*neighbors*). Uzly sledují své sousedy poslouchání *HELLO* zpráv, které uzel vysílá ve stanovených intervalech. Když jeden z uzlů potřebuje poslat zprávu jinému uzlu, který není jeho soused, tak vysílá (*broadcast*) žádost *Route Request (RREQ)*. RREQ zpráva obsahuje několik klíčových informačních bitů:

- Zdroj (*source*),
- cíl (*destination*),
- střední délku života zprávy (*lifespan*),
- pořadové číslo (*sequence number*), které slouží jako jedinečné ID.

Například (obrázek 4.2) uzel 1 si přeje odeslat zprávu uzlu 3. Jeho sousedy jsou však uzly 2 a 4, proto uzel 1 nemůže přímo komunikovat s uzlem 3 a posílá tedy RREQ. Zprávu RREQ slyší uzly 4 a 2.



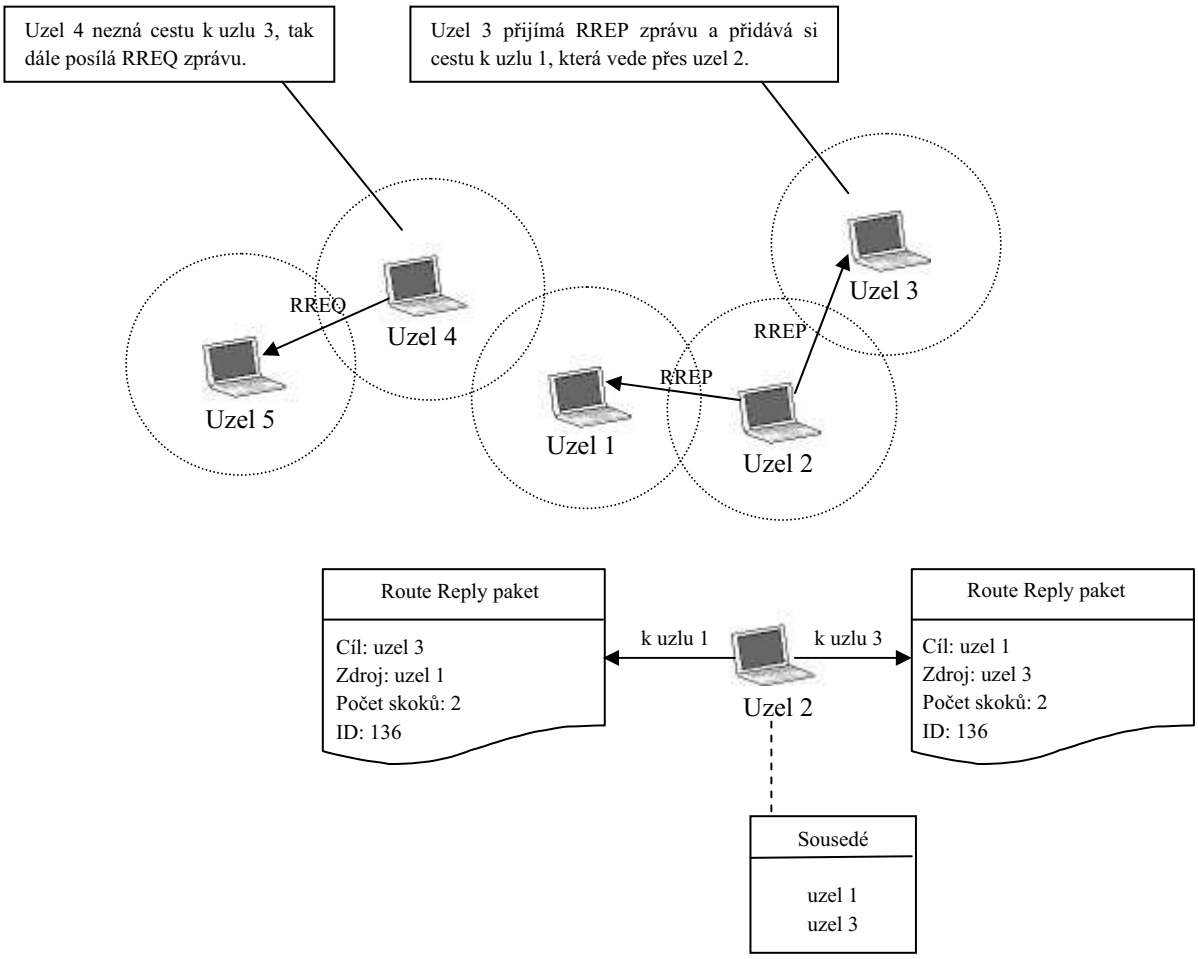
Obrázek 4.2 AODV směrování (RREQ)

Když sousedé uzlu 1 přijmou RREQ zprávu, mají dvě možnosti:

- Jestliže znají cestu k cíli, nebo oni sami jsou cíl, mohou poslat RREP (*Route Reply*) zprávu zpět uzlu 1,
- jestliže neznají cestu k cíli, tak přeposílají dále zprávu RREQ svým sousedům, dokud nevyprší střední délka života.

Jestliže uzel 1 nepřijme odpověď ve stanoveném čase, bude přeposílat žádost, ale tentokrát bude mít RREQ zpráva delší střední délku života a nové ID.

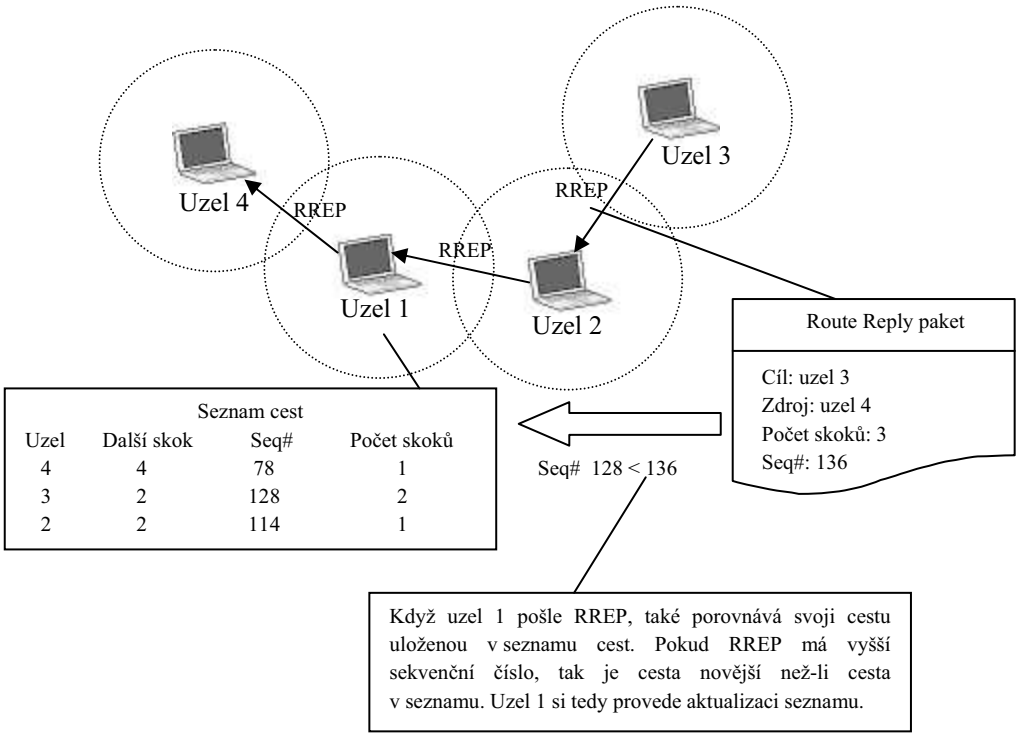
V příkladu (obrázek 4.3) uzel 2 zná cestu k uzlu 3 a odpovídá na RREQ posíláním RREP. Uzel 4 na druhé straně nezná cestu k uzlu 3, tak přeposílá RREQ.



Obrázek 4.3 AODV směrování (RREP)

Pořadové číslo (sequence number)

Pořadová čísla slouží jako časový údaj. Dovolují porovnávat, jak čerstvé jsou informace o jiných uzlech. Pokaždé, když uzel posílá nějaký typ zprávy, zvýší si tím vlastní pořadové číslo. Každý uzel si zaznamenává pořadové číslo všech ostatních uzlů, se kterými komunikuje. Vyšší pořadové číslo znamená čerstvější cestu. Toto umožňuje uzlům zjistit, který z nich má přesnější informace. Na obrázku 4.4 uzel 1 posílá RREP uzlu 4. Můžeme si všimnout, že cesta v RREP má lepší pořadové číslo, než cesta ve směrovací tabulce. Uzel 1 si poté aktualizuje informaci.



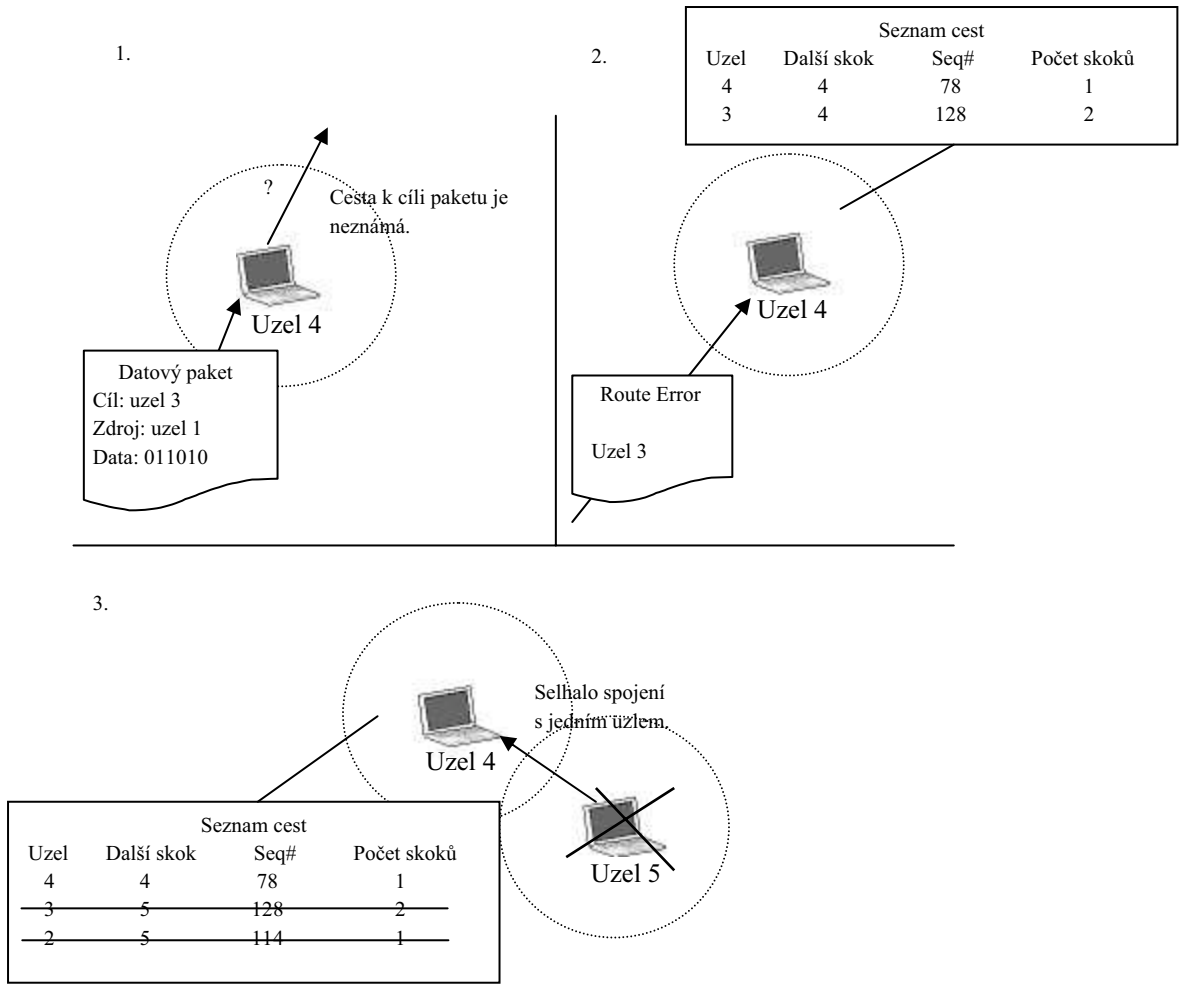
Obrázek 4.4 AODV – pořadová čísla

Chybové zprávy

RERR (*Route Error Message*) dovolují AODV přizpůsobovat cesty, když se uzly pohybují. Vždy, když uzel přijme RERR dívá se do své směrovací tabulky a odstraňuje všechny cesty, které obsahují špatné uzly.

Obrázek 4.5 ilustruje tři okolnosti, kdy uzel vysílá RERR svým sousedům.

- První scénář, kdy uzel přijímá datový paket, který chce poslat dále, ale nezná cestu k cíli. Skutečným problémem není, že uzel nezná cestu, ale že nějaký další uzel si myslí, že správná cesta k cíli je přes tento uzel.
- V druhém scénáři uzel přijímá RERR, která způsobí zrušení nejméně jedné cesty. Jestliže se tak stane, uzel posílá RERR se všemi novými uzly, které jsou nyní nedostupné.
- Ve třetím scénáři uzel zjistí, že nemůže komunikovat s jedním ze svých sousedů. Když se tak stane, podívá se do své směrovací tabulky a cestu, která používá souseda, jako další skok označí jako nevhodnou. Pak posílá RERR se sousedy a nevhodnými cestami.



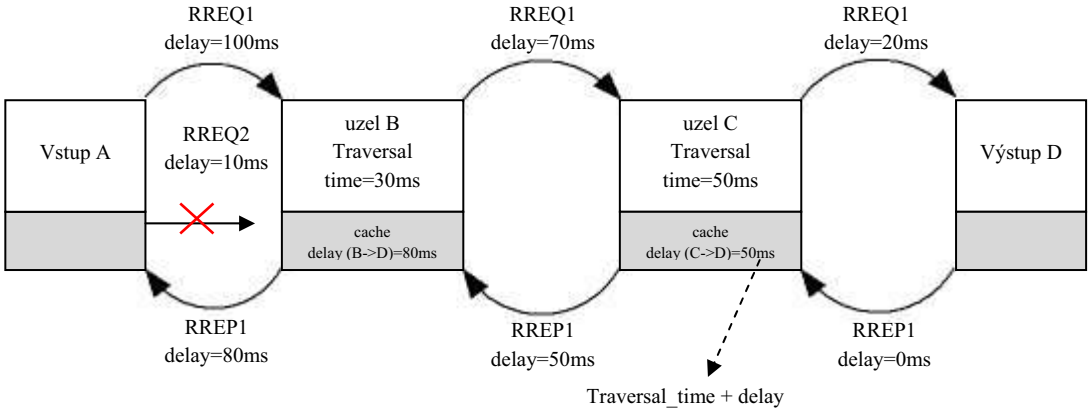
Obrázek 4.5 AODV směrování (RERR)

4.1.3 ROZŠÍŘENÍ AODV O PODPORU QOS – QOS AODV

Základní představa QoS AODV spočívá v rozšíření zpráv RREQ a RREP během fáze hledání cesty. Uzel, který přijímá RREQ s rozšířením o QoS musí být schopen splnit požadavky k tomu, aby buď přeposlal RREQ (jestli nemá aktualizovánu cestu ve své paměti), nebo poslal RREP ke zdroji. Jestli po sestavení takové cesty nějaký uzel podél cesty detekuje, že požadované QoS parametry nemohou být déle udrženy, tak uzel musí vytvořit ICMP QOS_LOST zprávu a vrátit ji ke zdroji.

Jak jsem se zmínil na začátku, je potřeba několik rozšíření ve směrovací tabulce RREQ a RREP zprávách pro podporu QoS směrování. AODV směrovací tabulka obsahuje následující pole, cílové pořadové číslo (*destination sequence number*), rozhraní (*interface*), počet skoků (*hop count*), další skok (*next hop*), seznam předchůdců (*list of precursors*). Navíc k těmto položkám pro QoS, AODV přidává další čtyři elementy, které jsou přidány k vlastnostem každé cesty. Tyto rozšíření jsou maximální zpoždění, minimální dostupná šířka pásma, seznam zdrojů vyžadujících záruky zpoždění a seznam zdrojů vyžadujících garanci šířky pásma.

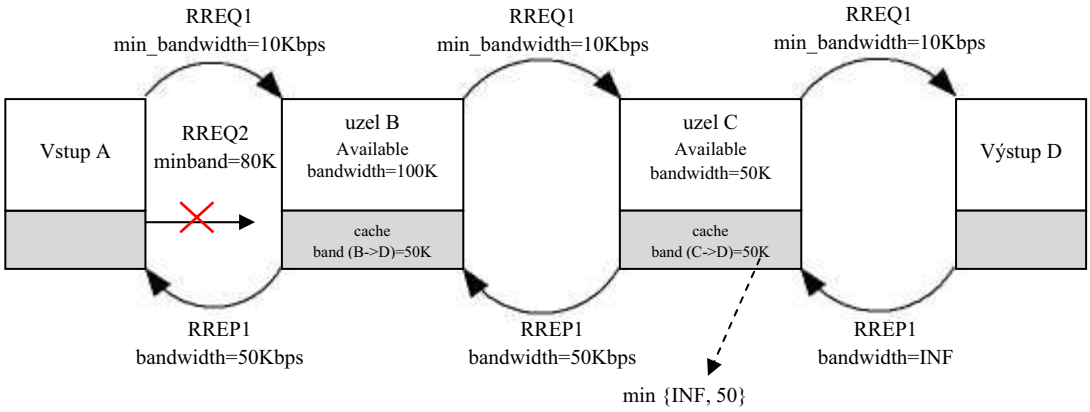
Maximální zpoždění signalizuje maximální množství sekund pro přenos ze zdroje (nebo z mezilehlého uzlu posílajícího RREQ) do cíle. Vždycky uzel přijímá RREQ ze kterého odečítá (od zpoždění indikovaného v RREQ) čas průchodu uzlu (*node traversal time*), což je čas požadovaný uzlem ke zpracování RREQ. Čas průchodu uzlu je defaultně nastaven na 40 ms, ale mohl by mít různou hodnotu, v případě, kdy tento uzel má více nebo méně energie. Jestli je čas průchodu uzlu větší než doba zpoždění indikovaná v RREQ, tak uzel jednoduše vyřadí RREQ a dále nezpracovává. Grafické znázornění na obrázku 4.6 ukazuje, jak RREQ1 bylo předáno prostředním (*core*) uzlům během procesu hledání cesty. V každém kroku je zpožďovací pole v RREQ sníženo o čas průchodu uzlu. Na konci uzel D odpoví RREP zprávou, která bude mít počáteční hodnotu zpoždění 0. Tato hodnota bude přidána k času průchodu každého uzlu a uložena ve směrovací tabulce pro další RREQ zprávy. Paměť hodnot zpoždění dělá z hledání cesty jednoduchý úkol. Například budoucí RREQ2 zpráva bude přímo zahozena uzlem B, protože požaduje zpoždění 10 ms a povolené zpoždění je 80 ms.



Obrázek 4.6 Posílání nebo vyřazení RREQ v závislosti na požadavku zpoždění

Postupem času může nastat situace, kdy například uzel C může zvýšit své zatížení, které by změnilo čas průchodu uzlu z 50 ms na 100 ms. Tato změna by ovlivnila veškeré závislé uzly, jako uzel B a A. Z tohoto důvodu uzel C posílá ICMP QOS_LOST zprávu všem potencionálním uzlům. To je také důvod proč si každý uzel na počátku ukládá seznam závislých uzlů (seznam zdrojů vyžadujících záruky zpoždění).

Minimální dostupná šířka pásma je pole, které signalizuje požadované množství šířky pásma pro specifické spojení (cestu). Při každém přijetí RREQ musí uzel porovnávat jeho dostupnou spojovací kapacitu s kapacitou (šířkou pásma) požadovanou v RREQ (viz obrázek 4.7). Jestli požadovaná šířka pásma není dostupná, pak uzel podobně jako u zpoždění RREQ jednoduše vyřadí a dále nezpracovává. Pokud je šířka pásma k dispozici, pak žádost bude zpracována, dokud je dosažitelný výstupní uzel. V tomto bodě výstupní uzel D bude odpovídat RREP zprávou, která bude inicializovat šířku pásma rovnou neurčité hodnotě (velice velké číslo). Každý uzel zasílající RREP srovnává pole šířka pásma v RREP a jeho vlastní spojovací kapacitu. Tato hodnota šířky pásma bude uložena ve směrovací tabulce pro budoucí RREQ. Paměť hodnot šířky pásma dělá z hledání cesty jednoduchý úkol. Můžeme se opět podívat na RREQ2 zprávu, která nebude uspokojena, protože požaduje 80 Kbps, což překračuje dostupných 50 Kbps.



Obrázek 4.7 Posílání nebo vyřazení RREQ v závislosti na požadované šířce pásma

Podobně jako u zpoždění i zde může uzel v budoucnu snížit spojovací kapacitu, která povede ke generaci ICMP QOS_LOST zprávy všem potencionálně ovlivněným uzlům. Seznam uzlů, které jsou ovlivněny touto vlastností je uložen v seznamu zdrojů požadujících garanci šířky pásma.

4.1.4 DSR (DYNAMIC SOURCE ROUTING)

DSR je reaktivní protokol, který může řídit MANET síť bez použití periodických aktualizací, jako tabulkou řízené směrovací protokoly. DSR byl navržen speciálně pro použití v *multi-hop* bezdrátových Ad hoc sítích. Ad hoc protokol dovoluje síti být zcela samo-organizovanou a samo-konfigurující, což znamená, že není potřeba existence žádné síťové infrastruktury nebo administrativy.

Proces hledání cesty je vykonáván pouze na základě požadavku uzlu (*on-demand* směrování). DSR odesilatel (zdroj, iniciátor) určuje celou cestu od zdroje k cílovému uzlu (*Source Routing* – zdrojové směrování) a ukládá adresy mezilehlých uzlů v cestě paketů. Ve srovnání s dalšími reaktivními směrovacími protokoly jako ABR nebo SSA, je DSR *beacon* menší, což znamená, že nejsou potřeba žádné *HELLO* pakety mezi uzly k oznámení sousedům o své přítomnosti. DSR byl vyvinut pro MANET s malým průměrem mezi 5 a 10 skoky (*hop*) a uzly by se měli pohybovat jen mírnou rychlostí.

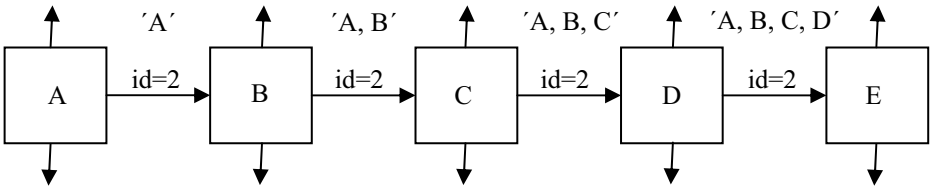
DSR je založený na *link state* algoritmu, což znamená, že každý uzel je schopen uložit si nejlepší cestu k cíli. V případě nějaké změny v topologii sítě, pak celá síť dostane tyto údaje formou záplavy.

DSR obsahuje dvě fáze:

- Nalezení cesty,
- údržba cesty.

Obě fáze jsou volány pouze na požádání.

Nalezení cesty

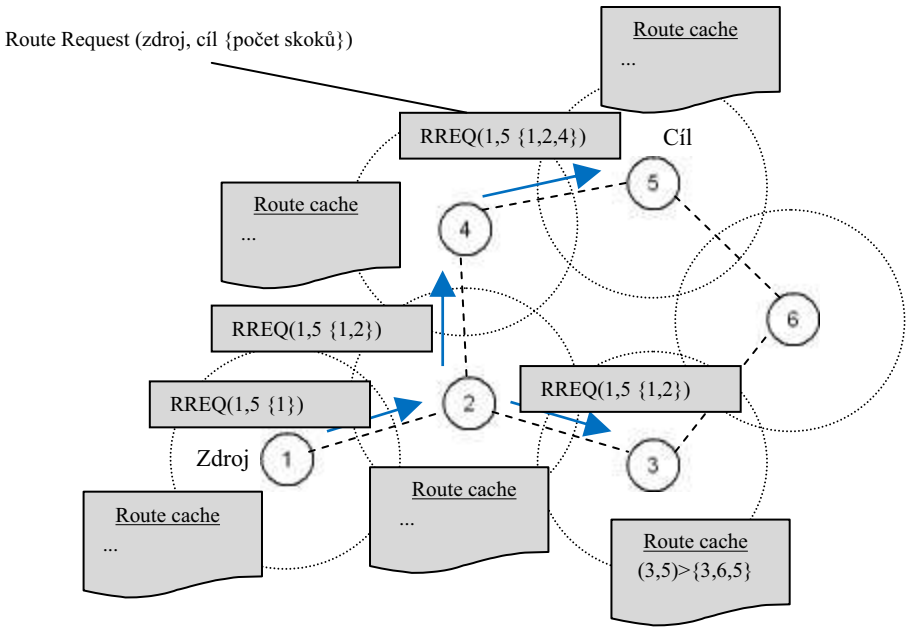


Obrázek 4.8 DSR fáze hledání cesty [9]

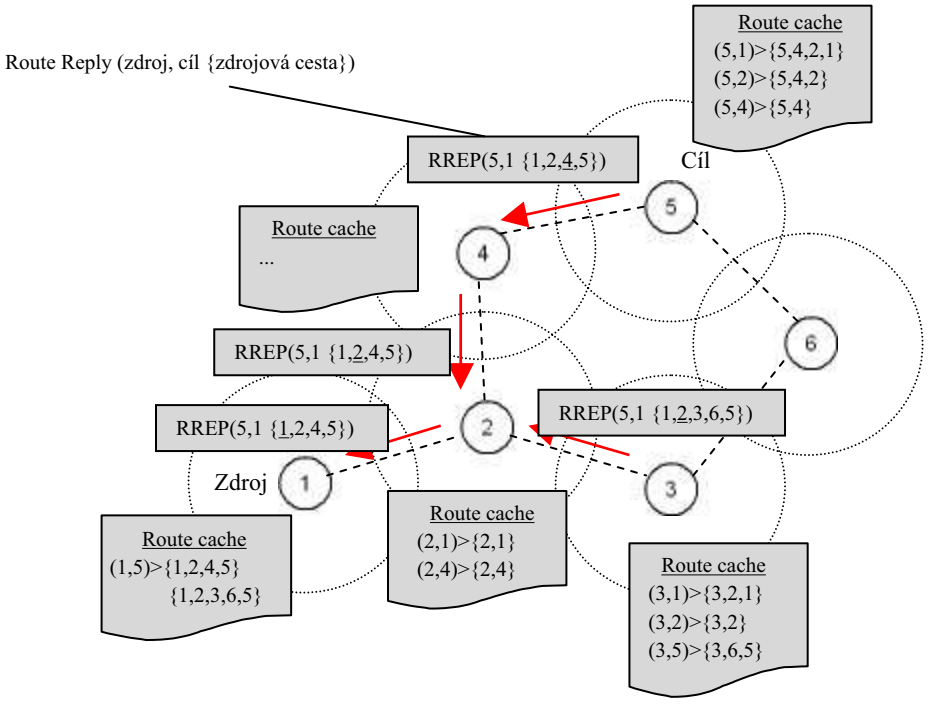
Jestliže uzel A má ve své paměti cestu k cíli (uzlu E), je tato cesta ihned použita. V opačném případě je zahájena fáze hledání cesty (obrázek 4.8):

- Uzel A (iniciátor) posílá *Route Request* pakety formou záplavy do sítě.
- Jestli uzel B v poslední době viděl jiný *Route Request* paket ze stejného cíle, nebo adresa uzlu B je již uvedena v *Route Record*, pak uzel B žádost zahodí.
- Je-li uzel B cílem, tak vrací *Route Reply* paket k uzlu A. *Route Reply* obsahuje seznam nejlepších cest od iniciátora k cíli. Když iniciátor přijímá tyto *Route Reply* pakety, uloží si tuto cestu do své paměti k následnému posílání paketů k cíli.

- Jinak uzel B není cílem a posílá, *Route Request* svým sousedům (kromě iniciátora).



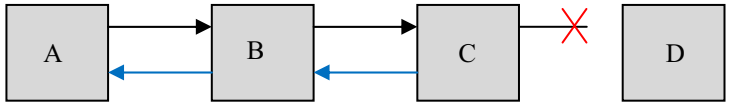
Obrázek 4.9 DSR RREQ



Obrázek 4.10 DSR RREP

Údržba cesty

V DSR je každý uzel zodpovědný za potvrzení, který další skok (uzel) ve zdrojové cestě přijímá pakety. Také každý paket je posílán pouze jednomu uzlu (*hop-by-hop* směrování). Jestli paket nemůže být uzlem přijat, je opětovně posílán vícekrát, dokud není přijato potvrzení od dalšího uzlu. Opětovný přenos může mít za následek selhání, *Route Error* zpráva je posílána ke zdroji, který tak může odstranit cestu ze své paměti.



Obrázek 4.11 DSR Route Error [9]

Jestliže uzel C nepřijímá potvrzení od uzlu D po nějakém množství žádostí, tak posílá *Route Error* k iniciátoru A (obrázek 4.11). Jakmile uzel přijme, *Route Error* paket, smaže si rozbitou cestu ze své paměti. Pokud má A další cestu k D, tak posílá pakety ihned použitím této nové cesty. Jinak uzel A startuje proces hledání znova.

Výhody

Reaktivní protokoly nemají potřebu pravidelně zaplavovat síť aktualizací směrovacích tabulek, jako směrovací protokoly řízené tabulkou. Mezilehlé uzly jsou schopny efektivně využívat informace z paměti a tím redukovat režie. Iniciátor se snaží najít cestu, pouze když není žádná cesta známa (uložena v paměti). Šetří se tak šířka pásma, protože nejsou posílány žádné *HELLO* pakety.

Nevýhody

Údržba cesty neopraví rozbité cesty. Rozbitá cesta je oznámena pouze zdroji. DSR protokol pracuje efektivně pouze v sítích, které mají méně než 20 uzlů. Problémy se také objevují, jestli se většina uzlů pohybuje příliš rychle, takže se uzly mohou pohybovat pouze mírnou rychlostí. Využití záplavy v síti může způsobit kolize mezi pakety. Také zde vzniká malé zpoždění na počátku nového spojení, protože iniciátor musí nejprve najít cestu k cíli.

4.1.5 OLSR (OPTIMIZED LINK STATE ROUTING PROTOCOL)

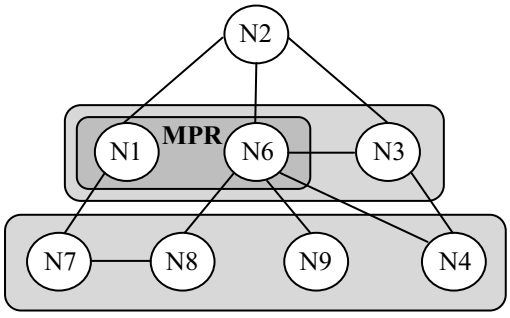
OLSR patří do skupiny proaktivních směrovacích protokolů, které se vyznačují tím, že informace potřebné ke směrování k jednotlivým uzlům jsou zjišťovány ještě před vznikem požadavku [11]. Což má za následek minimalizaci zpoždění při nově vzniklé komunikaci, ale na druhou stranu vzniká vyšší zatížení sítě režijními informacemi a vyšším výpočetním výkonem.

Každý uzel v síti pravidelně posílá *HELLO* a *Topology Control* (*TC*) pakety. *HELLO* pakety zjišťují informace o sousedních uzlech, o jejich vlastnostech a možnostech. Informace obsahují IP adresu uzlu, pořadové číslo (*sequence number*) a seznam informací o vzdálenosti k sousedním uzlům. Tyto informace jsou pak pomocí *TC* sdělovány ostatním uzlům v síti. Všechny uzly v síti si na základě těchto informací o sousedních uzlech tvoří informační databázi a směrovací tabulku. Ve směrovacích tabulkách uzly ukládají informace o cestách ke každému uzlu v síti. Informace jsou aktualizovány:

- Při detekci změny v sousedství uzlu,
- selhala-li cesta k některému z uzlů,
- je objevena lepší (kratší) cesta k cíli.

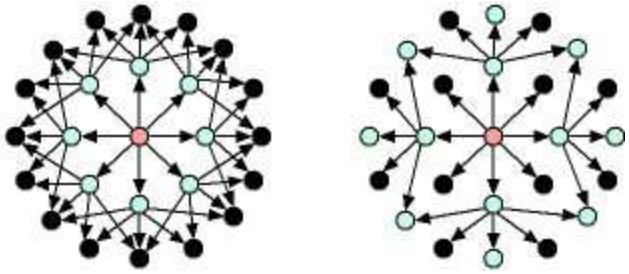
Rozdíl OLSR od LSR (*Links State Protocol*) je ten, že OLSR se spoléhá na funkci tzv. MPR (*multi-point relays*). MPR je uzel, který je vybrán jeho přímým sousedem (jeden skok). Účelem MPR je minimalizace záplavou vysílaných zpráv v síti. Informační paket by neměl být posílán ve stejné oblasti sítě dvakrát. MPR pomáhá redukovat a optimalizovat tento problém. Každý uzel informuje své sousedy (jeden skok vzdálené) o jeho MPR v *HELLO* paketech. Dalším z účelů je snížení velikosti *HELLO* paketů.

Každý uzel v síti (obrázek 4.12), v našem případě uzel N2, si vybere několik sousedních uzlů v síti. Tyto uzly budou posílat uzlu N2 pakety. Tyto vybrané uzly, N1 a N6 jsou nazývány MPR uzlu N2. Uzel N2 vybral své MPR k pokrytí všech uzlů, které jsou vzdáleny přesně dva skoky od něj. V našem případě N7, N8, N9 a N4. Uzel, který není MPR, může číst pakety posílané z N2, ale nemůže je posílat.



Obrázek 4.12 OLSR – výběr MPR

Na obrázku 4.13 vlevo je znázorněno posílání zpráv formou záplavy a vpravo zasílání s využitím *multi-point relays* MPR, kdy je patrné, že pouze MPR mohou posílat pakety vpřed (uzly, které mají světlou barvu).



Obrázek 4.13 Multi-point relays (MPR)

Výhody

- Minimální zpoždění,
- ideální pro použití ve velkých sítích a v sítích s velkou hustotou,
- OLSR dosahuje větší efektivity, než klasické *link state* algoritmy, v případě hustých sítí,
- OLSR se vyhýbá extra práci s hledáním cíle a udržováním směrovacích vstupů pro každý z cílů po celou dobu, takto poskytuje nízké přenosové zpoždění pro pakety,
- OLSR může být snadno rozšířen o podporu QoS.

Nevýhody

- Je-li síť řídká, každý soused uzlu se stává MPR,
- vysoký kontrolní provoz (režie), redukovány použitím MPR,
- vyšší výpočetní požadavky,
- složitější implementace.

4.1.6 ROZŠÍŘENÍ OLSR O PODPORU QOS – QOLSR

QOLSR je rozšíření protokolu OLSR o podporu QoS požadavků. Dodatečná pole pro QoS jsou přidána k *HELLO* a *TC* zprávám. Žádné další řídící zprávy nejsou vytvářeny. V QOLSR uzel měří QoS metriky jako dostupná šířka pásma, zpoždění, jitter atd., na spojeních ke svým sousedům. Tyto informace o QoS metrikách jsou užívány k počítání QoS – MPR (QMPR) a poté formou záplavy v síti *TC* zprávami počítána směrovací tabulka.

QOLSR cesty obsahují pouze QMPR, jako mezilehlé uzly mezi zdrojem a cílem. Pro výběr MPR, QOLSR vyžaduje stejnou heuristiku užívanou pro výběr MPR v OLSR. Tato heuristika redukuje záplavou vysílané pakety v síti minimalizováním opětovných přenosů.

QOLSR je proaktivní QoS směrovací protokol pro MANET sítě, jehož výhoda je, že má optimální cesty ihned dostupné, když jsou potřeba a to z důvodu své proaktivní povahy. QOLSR poskytuje koncovou podporu QoS požadavků a minimalizuje vysílání (záplavou) kontrolního provozu použitím pouze vybraných uzlů, nazvaných MPR k opětovnému vysílání řídících zpráv. Tato technika významně redukuje počet opětovných přenosů požadovaných k záplavě zpráv všem uzlům v síti. QOLSR provádí různé funkce, které jsou potřeba k vykonání směrování [12] :

Snímání spojení (*Link Sensing*)

Snímání spojení je realizováno periodickým vysíláním *HELLO* zpráv přes rozhraní, která kontrolují konektivitu. *HELLO* zpráva je generována separátně pro každé rozhraní. Výsledkem snímání je informace popisující spojení mezi místními rozhraními a vzdálenými rozhraními (tj. rozhraní k sousedním uzlům). Je-li poskytnuta dostatečná informace spojovací vrstvou, tak může být využita namísto výměny *HELLO* zpráv.

Měření QoS spojení (*Link QoS Measurement*)

Každý uzel musí odhadovat QoS parametry (dostupnou šířku pásma, zpoždění, cenu, bezpečnost, spotřebu energie atd.) na spojeních ke každému rozhraní souseda.

Detekce sousední a nejlepší QoS podmínky

V síti s pouze jedním rozhraním pro uzel, může uzel odečítat sousedy a nejlepší QoS podmínky přímo z vyměňovaných informací, jako součást snímání spojení.

Výběr MPR (*Multi-point Relay Selection*)

Každý uzel vybírá své MPR mezi jeden skok vzdálenými sousedy. MPR jsou vybírány tak, aby pokrývaly (v rámci rozsahu) veškeré uzly vzdáleny dva skoky. Informace požadovaná k vykonání tohoto výpočtu je získána periodickou výměnou *HELLO* zpráv. MPR jsou přepočítávány, když dojde ke změně mezi uzly vzdálenými 1 popř. 2 skoky.

QoS MPR (QMPR)

Každý uzel v síti nezávisle vybírá svoji vlastní sadu QMPR. Tato sada je vypočítána tak, aby obsahovala podmnožinu jeden skok vzdálených sousedů, kteří poskytují nejlepší QoS záruky od každého dva skoky vzdáleného souseda k danému uzlu. QMPR sada nepotřebuje být optimální, avšak měla by dostatečně minimalizovat vytváření *TC* zpráv v síti. Informace potřebné k vykonání takového výpočtu jsou získány periodickou výměnou *HELLO* zpráv. QMPR daného uzlu jsou deklarovány v následující *HELLO* zprávě přenášené tímto uzlem. QMPR sada je přepočítána dojde-li ke změně mezi uzly vzdálenými 1 popř. 2 skoky, nebo je objevena změna v QoS podmínce.

QMPR a deklarace nejlepší QoS podmínky (*QMPR and Best QoS Conditions Declaration*)

TC zprávy jsou posílány každým QMPR uzlem v síti v pravidelných intervalech k deklaraci svých QMPR voličů a QoS podmínky. Informace přenášené těmito zprávami v síti pomáhají každému uzlu sestavovat svojí směrovací tabulku.

Sestavení (výpočet) směrovací tabulky (*Routing Table Calculation*)

Každý uzel udržuje směrovací tabulku, která mu dovoluje směrovat pakety k cílům v síti s optimální metrikou respektující QoS omezení.

4.1.7 TORA (TEMPORALLY – ORDERED ROUTING ALGORITHM)

TORA je adaptivní směrovací protokol pro *multi-hop* sítě, které mají následující atributy [10]:

- Distribuovanou povahu,
- směrování bez vzniku smyček,
- vícecestné směrování,
- reaktivní nebo proaktivní organizace a údržba cesty,
- minimalizace kontrolních informací.

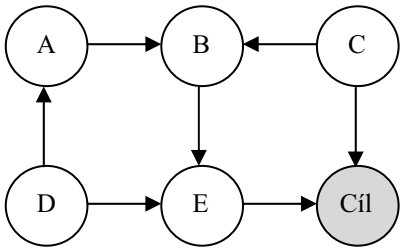
TORA je distribuovaný v tom, že router potřebuje udržovat pouze informace o sousedních routerech (tj. znalost jednoho skoku) [10]. TORA si udržuje stav na základě cíle. Avšak nevykonává výpočet nejkratší cesty a tak metrika používaná ke směrování nepředstavuje vzdálenost. Povaha směrování orientovaná na cíl podporuje směs reaktivního a proaktivního směrování. Během reaktivní činnosti zdroje zahajují organizaci cesty k danému cíli na požádání. Tento druh činnosti může být výhodný v dynamických sítích s relativně slabým provozem. Nesmí být nutné (ani žádoucí) udržovat vždy cesty mezi každým párem zdroj cíl. Zároveň vybrané cíle mohou zahájit proaktivní operace, podobné tradičnímu tabulkou řízenému přístupu. Toto dovoluje udržování cest k cíli, pro které je často požadováno směrování (např. servery nebo brány do pevné sítě).

TORA je navržen k minimalizaci režijních informací s přizpůsobením sítě ke změnám topologie. Rozsah řídících zpráv je typicky lokalizovaný k velmi malému množství uzlů blízkému změně topologie.

TORA pracuje na vrcholu nižší vrstvy, nebo protokolu, který poskytuje následující základní služby mezi sousedními routery:

- Snímání stavu spojení a objevení souseda,
- spolehlivé, bezchybné doručení paketů,
- bezpečné ověření.

TORA definuje jakési směrnice ke spojení mezi routery tvořící směrovací strukturu použitou k zasílání datagramů k cíli. Router přiřazuje směr (upstream nebo downstream) spojení se sousedním routerem na základě hodnot metriky přidružené routeru. Metrika routeru může být nazývána úroveň (výše) routeru (tj. spojení jsou směrována z vyššího routeru k nižšímu routeru). Význam výše a spojovacích režijních úkolů je takový, že router smí posílat datagramy pouze pro downstream. Spojení od routeru k sousednímu routeru s neznámou nebo nedefinovanou výší, jsou považována za nevhodné a nemohou se tedy účastnit komunikace. Souhrnně výše routerů a spojovací režijní úkoly tvoří směrovací strukturu, ve které všechny cesty vedou k cíli (obrázek 4.14). Můžeme si všimnout, že C je blíže k cíli než B v rámci množství skoků, ale metrika C (výše) je větší, než má B.



Úrovně (výše) routerů

H(C) > H(B) > H(E) > H(Cíl)

H(D) > H(A) > H(B) > H(E) > H(Cíl)

Obrázek 4.14 TORA – úroveň (výše)

TORA může být rozdělena na čtyři základní funkce [10]: vytvoření cesty, údržba cesty, mazání cesty a optimalizace cesty. Vytvoření cesty odpovídá výběru výší, které tvoří řízenou sekvenci spojení vedoucí k cíli v předtím neřízené síti, nebo části sítě. Údržba cesty se odkazuje na přizpůsobení směrovací struktury v odpovědi na změny topologie. Například ztráta spojení nějakého z routerů, což může vést k tomu, že cesta dočasně nevede k cíli. Tato událost spouští sekvenci událostí k opětovnému výběru výší routeru, které přeorientují směrovací strukturu tak, že cesta opět vede k cíli. V případech, kdy je síť rozdělena, spojení v části sítě, která je oddělena od cíle musí být označeno jako neřízené a smazáno. Nakonec TORA také obsahuje sekundární mechanismus pro optimalizaci cest, ve kterých routery znovu zvolí svoje výše, aby tak zlepšili směrovací strukturu. TORA vykonává tyto čtyři funkce pomocí čtyř kontrolních paketů, a sice dotaz (*query* – QRY), aktualizace (*update* – UPD), odstranit (*clear* – CLR) a optimalizace (*optimization* – OPT).

5. SIMULACE V OPNET MODELERU

5.1 OPNET MODELER

Jako prostředí pro tvorbu simulací je použit program OPNET Modeler (dále jen OM), který umožňuje návrh, analýzu a simulací sítí. Mezi jeho výhody patří možnost simulace rozsáhlých sítí, efektivnost, výkonnost a objemné knihovny s dostupným zdrojovým kódem.

Lze modelovat (simulovat) prakticky jakékoliv architektury sítí, ze kterých poté lze vytvořit různé statistiky pro analýzu sítě. OM nám také umožňuje ověřit chování reálného objektu v různých, i extrémních podmínkách, čímž můžeme předcházet nežádoucím stavům.

Výsledné statistiky lze generovat do formátu XML, HTTP nebo tabulek.

Simulační prostředí

- Verze simulačního programu: *OPNET Modeler 14.0.A PL1 (Build 6105)*.

Systém

- Typ OS: *Microsoft Windows XP Professional, verze 2002, SP 2.*

5.2 SIMULACE MANET SÍTĚ

K simulaci nám poslouží simulační program OPNET Modeler jehož vlastnosti jsou popsány v kapitole 5.1.

Při vytváření nového projektu byla zvolena mapa *Campus* s rozměry 10×10 kilometrů. Z nabídky *Model Family* byl vybrán model *MANET_toolbox* a *internet_toolbox,* který obsahuje jednotlivé komponenty potřebné pro tvorbu topologie sítě MANET. Z nabídky pro MANET byly pro jednoduchou simulaci použity následující:

- **Wireless LAN Server** – který může být konfigurován tak, aby podporoval některý ze směrovacích protokolů MANET a směroval pakety mezi klientem a serverem.
- **Wireless LAN workstation** – může taktéž podporovat některý ze směrovacích protokolů MANET a dále je schopna generovat aplikační provoz (FTP, e-mail, HTTP atd.).
- **Application config** – definuje aplikace.
- **Profile config** – definuje profil aplikace/í a také nabízí možnost nastavení, kdy se jaká aplikace bude spouštět, kolikrát se v sítí bude moci zopakovat atd.

Návrh sítě je znázorněn na obrázku 5.1. V *application_config* je nadefinována jedna aplikace, a sice FTP. V *profile_config* je vytvořen jeden profil s názvem FTP, kterému byla přiřazena nadefinovaná aplikace v *application_config*. Tento profil je poté přiřazen všem stanicím (uzlům) v síti. Důležité také je nastavit podporu pro zvolenou aplikaci na serveru. Po těchto nezbytných krocích je nutný výběr vhodných simulovaných statistik pro následnou analýzu sítě.

Výběr simulovaných statistik

Globální statistiky (*Global Statistics*)

- Wireless LAN Throughput – reprezentuje celkový počet bitů poslaných mezi všemi uzly v síti.
- Wireless LAN Delay – statistika ukazuje koncové zpoždění všech přijatých paketů v síti.

Statistiky jednotlivých uzlů (*Node Statistics*)

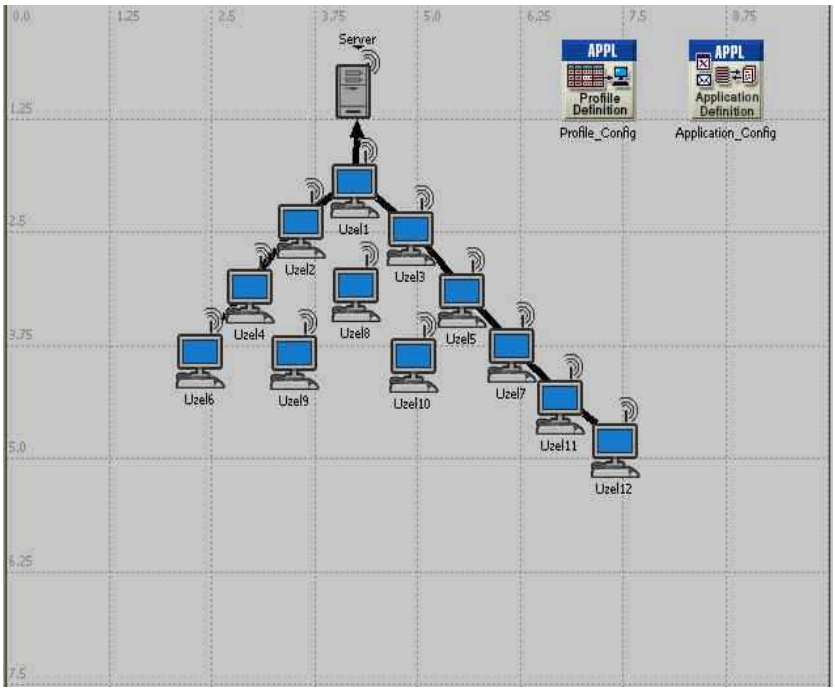
- Server FTP Load – rychlost, jakou přicházejí FTP žádosti na server.

Parametry simulace

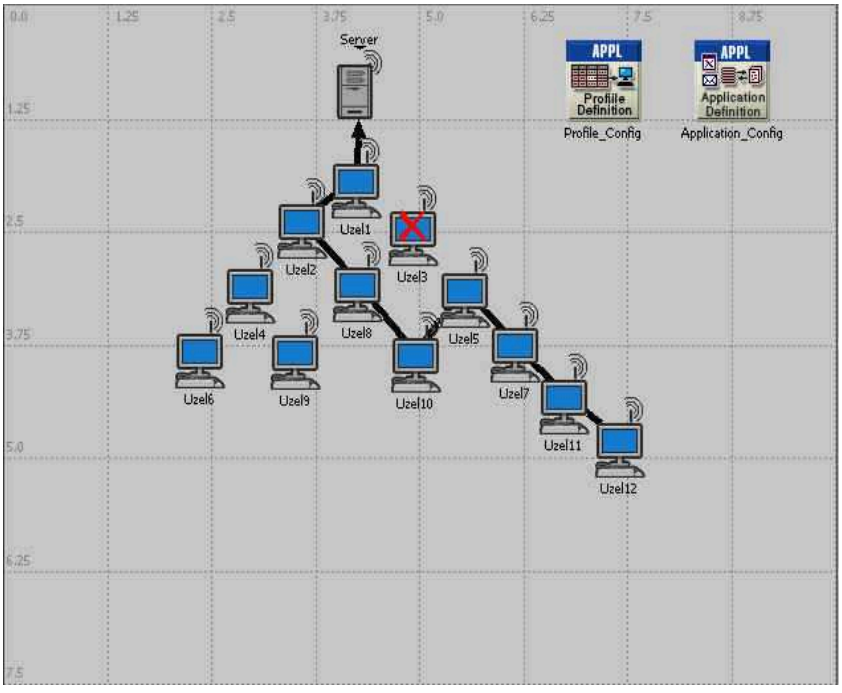
- Doba trvání – 1 hodina.
- Počet událostí – 300.
- Simulovány byly všechny scénáře najednou.

Simulované scénáře

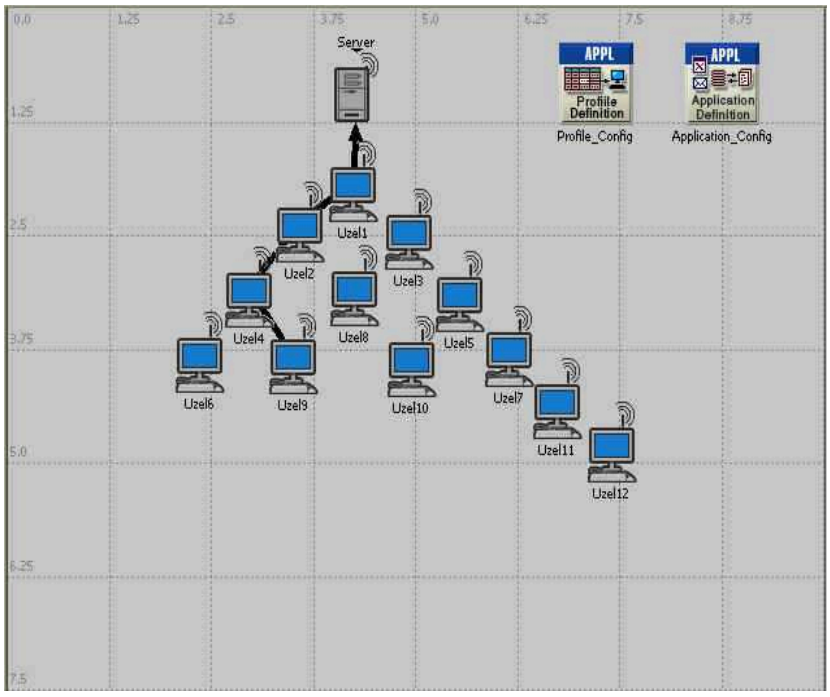
- **První scénář** (obrázek 5.1) – ukazuje topologii sítě a znázorňuje cesty, kterými komunikují vzdálenější uzly se serverem. Z cest je patrné, že vzdálené uzly nekomunikují se serverem přímo, nýbrž skoky přes ostatní uzly.
- **Druhý scénář** (obrázek 5.2) – znázorňuje tutéž topologii, ale jeden z uzlů selhal (červený křížek). Je zde vidět nalezení alternativní cesty při výpadku uzlu.
- **Třetí scénář** (obrázek 5.3) – opět je použita stejná topologie, s tím rozdílem, že jeden z uzlů je mobilní přiřazením zvolené trajektorie (zelená šipka). Scénář ilustruje chování mobilního uzlu a nelezení alternativní cesty.



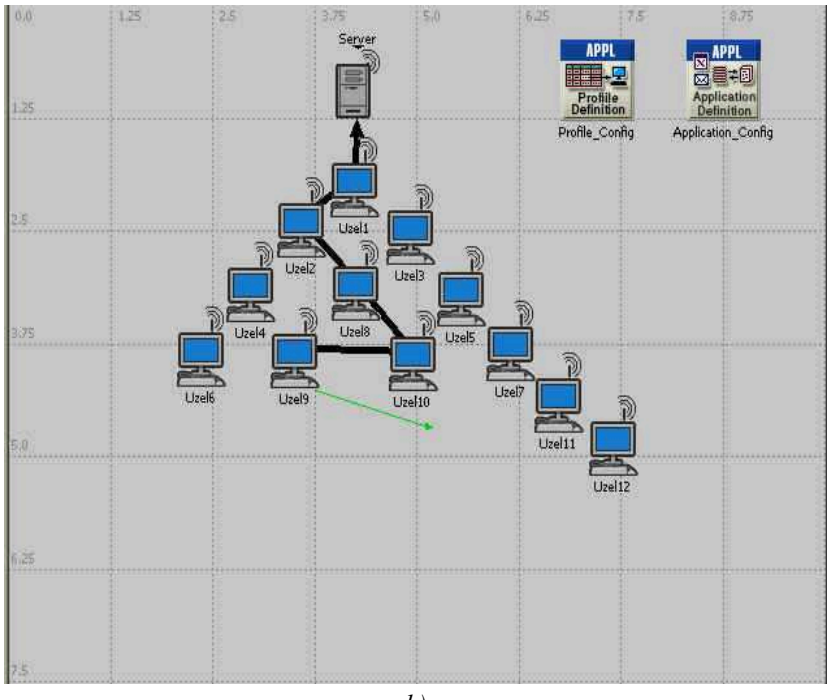
Obrázek 5.1 První scénář – topologie sítě



Obrázek 5.2 Druhý scénář – výpadek uzlu



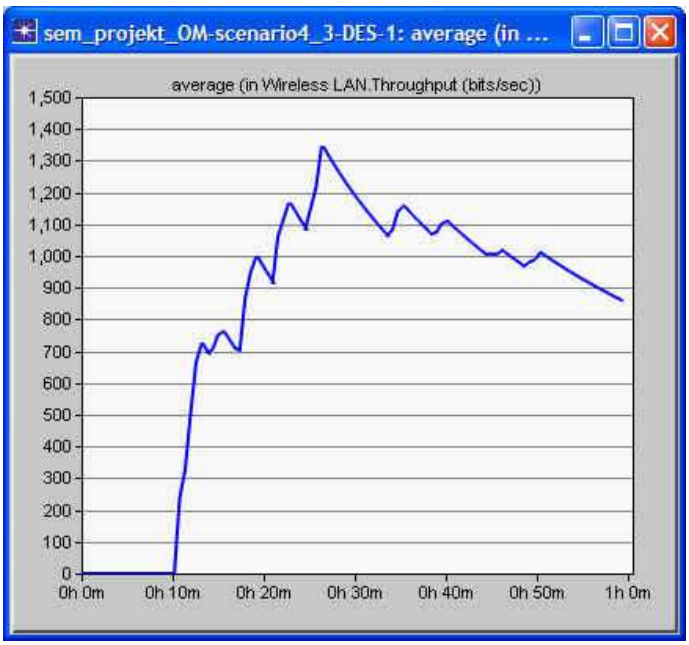
a)



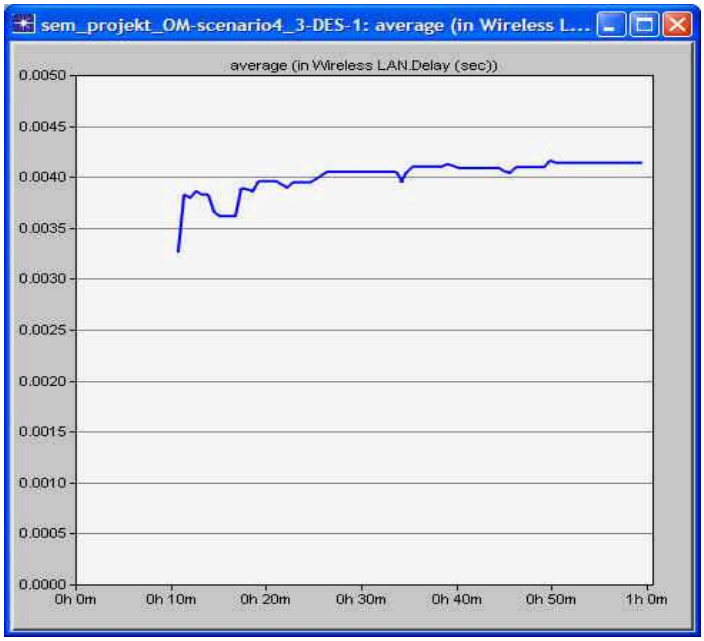
b)

Obrázek 5.3 Třetí scénář: a) původní cesta uzlu9, b) alternativní cesta uzlu9 pohybujícího se po trajektorii

Pro úplnost je nezbytné zde také uvést statistiky, které vznikly provedením simulace, a sice prvního scénáře. První statistika (obrázek 5.4) ilustruje celkovou výkonnost (propustnost) sítě a druhá statistika (obrázek 5.5) zobrazuje zpoždění v síti.



Obrázek 5.4 Výkonnost (propustnost) sítě



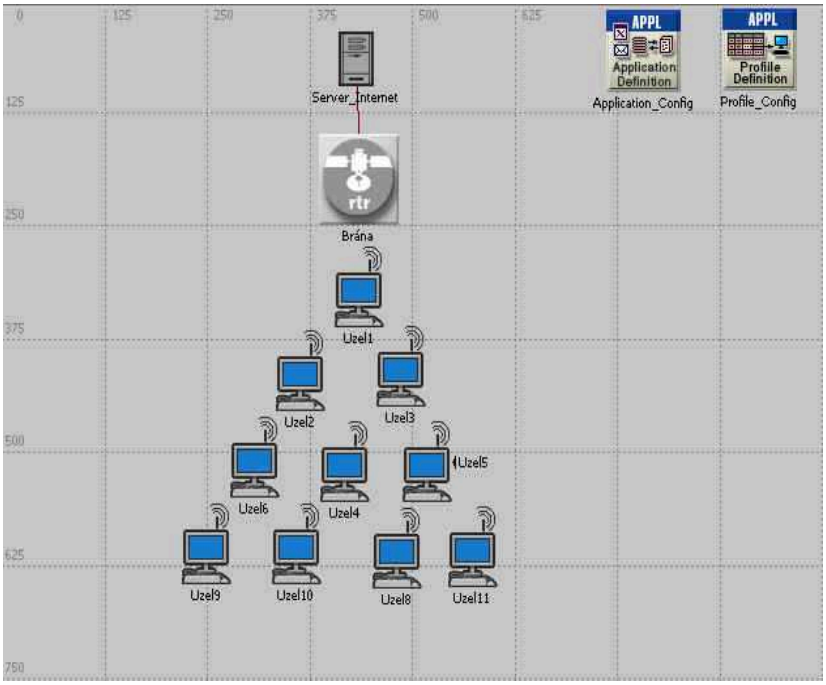
Obrázek 5.5 Zpoždění v síti

5.3 SIMULACE MESH SÍTĚ

K návrhu sítě byly z nabídky *Model Family* opět vybrány modely *MANET_toolbox* a *internet_toolbox*. Z těchto modelů byly použity následující komponenty:

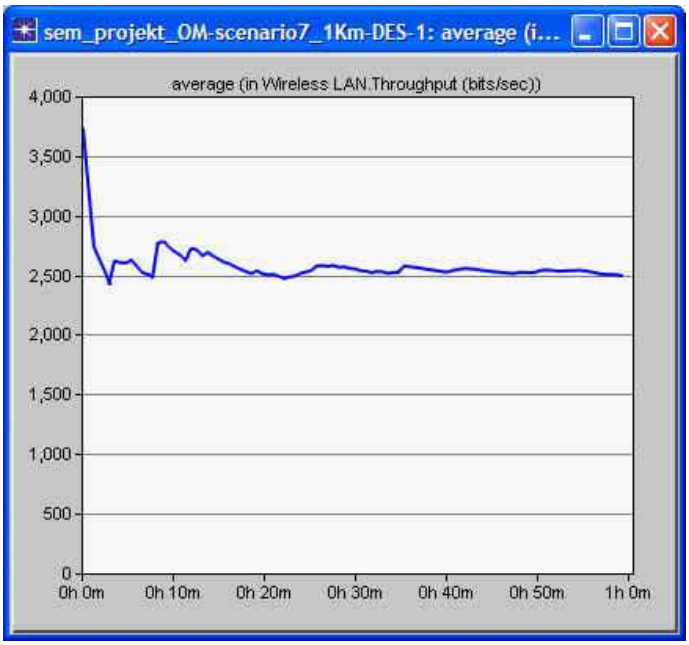
- **Application config** – viz kap. 5.2.
- **Profile config** – viz kap. 5.2.
- **Wireless LAN workstation** – viz kap. 5.2.
- **Ethernet Server**.
- **WLAN Ethernet router** – který obsahuje dvě rozhraní. Jedno rozhraní je pro WLAN a druhé rozhraní je pro ethernet.

Nastavení *application_config*, *profile_config* a zobrazovaných statistik je totožné jako v předešlé kapitole. Návrh sítě je vidět na obrázku 5.6.

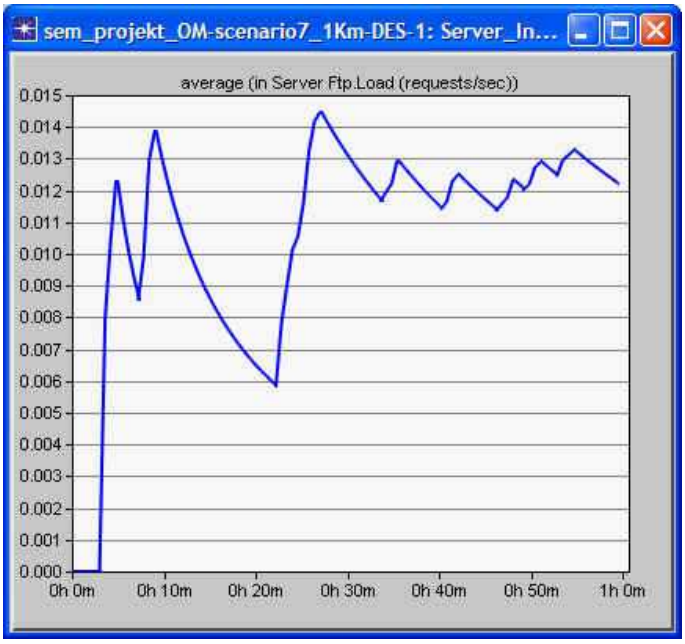


Obrázek 5.6 Návrh sítě

Brána (*WLAN Ethernet Router*) je jakýsi mezi uzel pro komunikaci s okolním světem. Jedno její rozhraní (*Ethernet*) je připojeno k serveru a druhé (*WLAN*) distribuuje komunikaci ostatním uzlům. Ze statistik, které vznikly simulací je uvedena globální statistika propustnosti (výkonnosti) sítě (obrázek 5.7) a statistika rychlosti s jakou přicházejí žádosti FTP na server (obrázek 5.8).



Obrázek 5.7 Výkonnost (propustnost) sítě



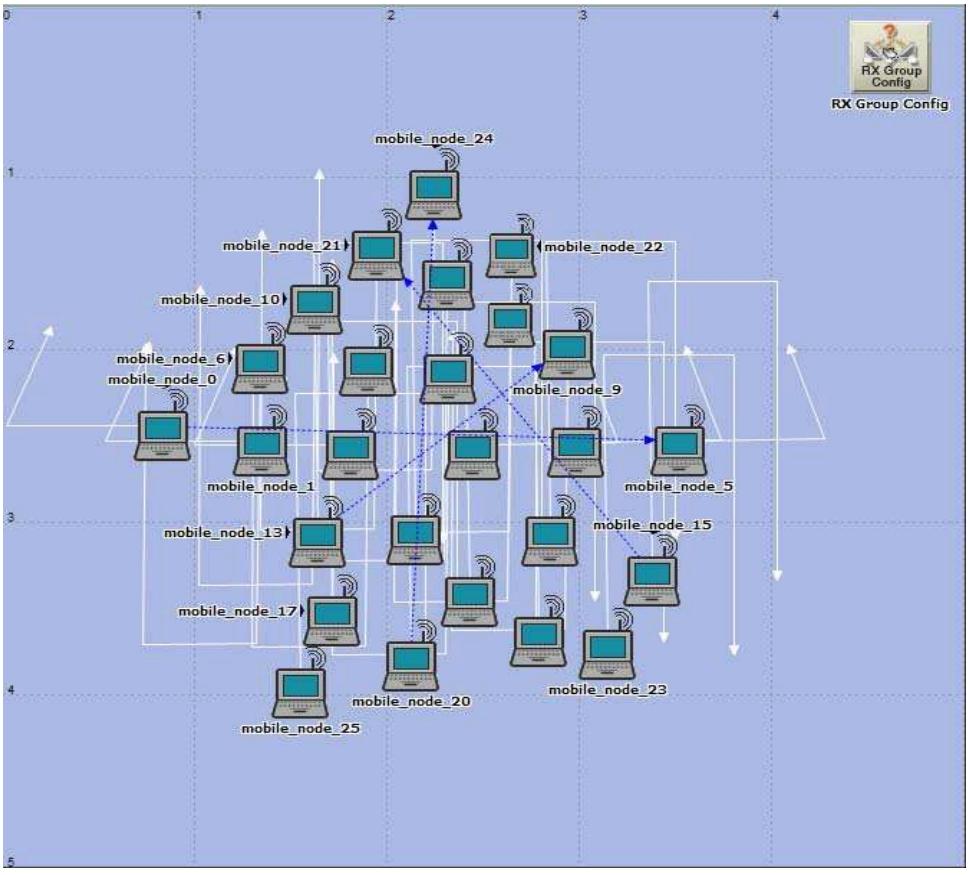
Obrázek 5.8 Rychlost jakou přicházejí žádosti FTP na server

5.4 SIMULACE SMĚROVACÍCH PROTOKOLŮ V MANET

Jako simulační prostředí byl opět použit simulační program OPNET Modeler, jehož význačné vlastnosti jsou popsány v kapitole 5.1. V této verzi programu jsou dostupné následující směrovací protokoly určené pro použití v MANET, a sice AODV, DSR, OLSR a TORA. Rychlost simulace je jednak ovlivněna nastavením samotného OM a také konfigurací počítače, kde byly simulace prováděny.

5.4.1 MODEL SÍTĚ

Model sítě na obrázku 5.9, na kterém budou simulovány a implementovány jednotlivé směrovací protokoly, byl vytvořen na prázdném scénáři o rozloze 5×5 kilometrů s použitím komponent umístěných v *MANET_toolboxu,* který byl zvolen na začátku při vytváření scénáře. Z těchto komponent jsou použity *manet_station* (*mobile_node 0* až *mobile_node 26*) a *RX_Group Config.* Nastavené jednotlivé parametry těchto komponent jsou uvedeny níže. Hodnoty ostatních parametrů jsou defaultní.



Obrázek 5.9 Model sítě

Typ provozu

Jako provoz je jednak využit režijní provoz samotných protokolů a dále provoz mezi jednotlivými uzly (modrá čárkovaná čára), který je realizován pomocí komponenty *ip_traffic_flow*. Z nabídky jednotlivých druhů provozu byl vybrán *IP_G711_Voice*.

Mobilita uzlů

Pohyb uzlů (bílá čára) je realizován přiřazením trajektorie každému z uzlů zvlášť. Jednotlivé trajektorie jsou vytvořeny pomocí nástroje *Define_Trajectory* (*Topology → Define Trajectory*). Doba trvání trajektorie je 16 minut.

Nastavené parametry *manet_station*

- **Ad hoc směrovací protokol** – vybrán vždy jeden z nabízených (AODV, OLSR, DSR, TORA).
- **Typ fyzikálního přenosu – kódování** – *Direct Sequence*.
- **Maximální rychlost přenosu** – *1 Mbps*.
- **Vysílací výkon vysílače** – *0,001 W*.
- **Citlivost přijímače** – *- 95 dBm*.

Nastavené parametry *RX_Group Config*

- RX_Group Config se využívá ke kalkulaci souboru možných přijímačů, se kterými může každý uzel komunikovat. Soubor možných přijímačů je omezen například na základě vzdálenosti (*Distance Threshold*).
- **Distance Threshold** – *700 m*: Tato volba bude omezovat přijímače mimo specifikovanou prahovou hodnotu vzdálenosti.

Nastavené parametry provozu *IP_G711_Voice*

- **Type of Service (ToS)** – *interaktivní hlas*.
- **Record Route Option** – *všechny pakety*: Specifikuje, zda zaznamenat cestu paketů od zdroje k cíli. Výstup je viditelný například v textovém formátu *(<proj - scen> conv_flow_routes.gdf*) viz příloha 1.
- **Traffic Mix** – *0,1% Explicit*: Tato volba určuje druh provozu generovaného požadavkem. Požadavek může generovat explicitní provoz (paket po paketu), provoz na pozadí nebo nějakou směs těchto provozů. Explicitní provoz generuje jednotlivé pakety, které reprezentují celkový objem požadavku. Výsledkem je velmi detailní reprezentace toku, ale prováděná simulace může být dosti dlouhá. Provoz na pozadí představuje provoz požadavku v celkové cestě. K tomu abychom následně mohli analyzovat zpoždění jednotlivých toků byla nastavena směs provozu. Tedy 0,1 % provozu je explicitní a zbytek na pozadí.
- **Traffic Start Time** – *2. minuta*: Specifikuje čas spuštění požadavků.

Výběr simulovaných statistik

Globální statistiky (*Global Statistics*)

- Výběr statistik konkrétního směrovacího protokolu (AODV, OLSR, DSR, TORA).

Statistiky jednotlivých uzlů (*Node Statistics*)

- Výběr statistik konkrétního směrovacího protokolu (AODV, OLSR, DSR, TORA).

Statistiky požadavků (*Demand Statistics*)

- Koncové zpoždění paketů (*Packet ETE Delay*). Čas mezi vytvořením paketu ve zdrojovém uzlu a jeho přijetím v cílovém uzlu.
- Kolísání zpoždění paketů (*Packet Jitter*). Rozdíl mezi koncovým zpožděním dvou po sobě jdoucích paketů.

Parametry simulace

- Doba trvání – 16 minut.
- Počet událostí – 300.
- Simulovány byly všechny scénáře najednou a výsledné statistiky jsou uvedeny v kapitole 5.4.4, kde je také provedena analýza těchto statistik z pohledu režijních informací potřebných pro směrování dat, koncového zpoždění jednotlivých paketů a kolísání zpoždění.

Vytvořený model sítě byl brán jako vzorový a byl použit ve všech ostatních simulovaných scénářích, které se liší v implementaci konkrétního směrovacího protokolu a ve výběru statistik odpovídajících danému protokolu. Tento postup byl zvolen proto, aby bylo možné následně všechny statistiky relevantně vyhodnotit z různých pohledů a říci, který ze směrovacích protokolů je nejvhodnější pro použití v takovéto MANET síti.

5.4.2 SIMULOVANÉ SCÉNÁŘE

Simulováno bylo celkem 5 scénářů, které jsou založeny na modelu sítě, který byl vytvořen v kapitole 5.4.1. Scénáře pro jednotlivé směrovací protokoly (Ad hoc) se liší pouze v jejich implementaci a jim odpovídajících statistikách. Z dostupných směrovací protokolů v OM byly simulovány následující:

- První scénář – AODV,
- druhý scénář – OLSR,
- třetí scénář – DSR,
- čtvrtý scénář – TORA.

V posledním pátém scénáři je ilustrována schopnost nalezení alternativní cesty v případě výpadku jednoho či několika uzlů. Níže jsou popsány nastavené parametry jednotlivých směrovacích protokolů a jejich krátká charakteristika. Hodnoty parametrů, které zde nejsou popsány jsou brány jako defaultní a nastaveny přímo OM.

Parametry AODV

- **Gratuitous Route Reply Flag** – *Enable*: Signalizuje, zda by měla být poslána Route Reply zpráva uzlu, který je specifikován v poli IP jako cíl, jestliže uzel posílající Route Reply není cíl.
- **Hello Interval** – *uniform (10,10.1)*: Tento parametr udává časový interval přenosu *HELLO* zpráv.
- **Allowed Hello Loss** – *3*: Volba definuje počet ztracených *HELLO* paketů, které může uzel tolerovat před označením spojení jako přerušené.
- **Active Route Timeout** – *3 sekundy*: Označuje dobu existence položky ve směrovací tabulce.

Parametry OLSR

- **Willingness** – *default*: Udává, jak ochotný je uzel posílat data ostatním uzlům. Ochotu uzlu lze nastavit na „nikdy ochotný“, kdy si uzel nepřeje přenášet data pro ostatní a „vždy ochotný“, kdy je uzel vždy ochoten přenášet data. Volba *default* je brána jako normální. Tento parametr je založen na dostupnosti zdrojů jako baterie, kapacita atd. pro jednotlivé uzly.
- **Hello Interval** – *2 sekundy*: Tento parametr specifikuje, jak často budou vysílány *HELLO* pakety, nezbytné k udržování souvislostí mezi sousedními uzly.
- **TC Interval** – *5 sekund*: Specifikuje, jak často budou vysílány *TC* zprávy, které jsou vytvářeny MPR a nesou informaci o topologii. Používají se pro výpočet směrovací tabulky.
- **Neighbor Hold Time** – *6 sekund*: Parametr vyjadřuje expiraci (vypršení) spojení a je typicky nastaven na trojnásobek Hello Intervalu a není-li v tomto intervalu přijat *HELLO* paket jistého spojení, je toto spojení označeno jako ztracené. S každým přicházejícím paketem je časovač resetován. Jestliže jsou všechna spojení k sousednímu uzlu označena jako ztracená, je uzel označen jako nedosažitelný.

Parametry DSR

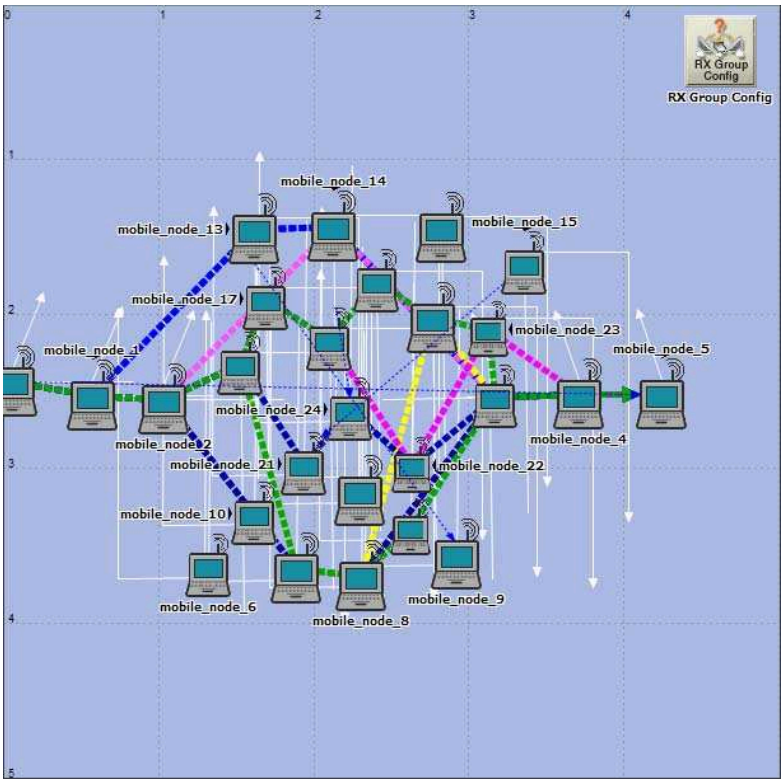
- **Route Cache Export** – *Export*: Export paměti směrování do výstupní tabulky. Ukázka části tabulky je dostupná v příloze 2.
- **Request Table Size** – *10 uzlů*: Udává maximální počet cílů (uzlů), které může tabulka žádostí udržovat.
- **Maximum Request Table Identifiers** – *16*: Maximální počet hodnot identifikace udržovaných v každé položce *Route Request* tabulky pro specifickou cílovou adresu.
- **Maximum Request Period** – *10sekund*: Po každém pokusu o nalezení cesty je interval mezi dalším hledáním pro tento cíl dvojnásobný, až do hodnoty uvedené v tomto parametru, dokud není přijata platná *Route Reply* zpráva od cíle.
- **Maximum Buffer Size** – *50 paketů*: Maximální velikost vyrovnávací paměti.

Parametry TORA

- **Mode of Operation** – *On Demand*: Specifikuje, v jakém režimu budou uzly v síti hledat cestu k dalším uzlům v síti. V režimu na požádání (*on demand*) budou uzly zaplavovat síť dotazy, když paket ještě nezná cestu k cíli. V proaktivním režimu (volba *proactive*) uzly pravidelně posílají OPT (optimalizační) pakety svým sousedním uzlům.
- **OPT Transmit Interval** – *300sekund*: V proaktivním režimu parametr specifikuje, jak často budou vysílány OPT pakety.
- **IP Packet Discard Timeout** – *10sekund*: Pokud nemůže být nalezena cesta, tak tento parametr určuje, jak dlouho bude paket ve frontě, předtím, než je vyřazen.

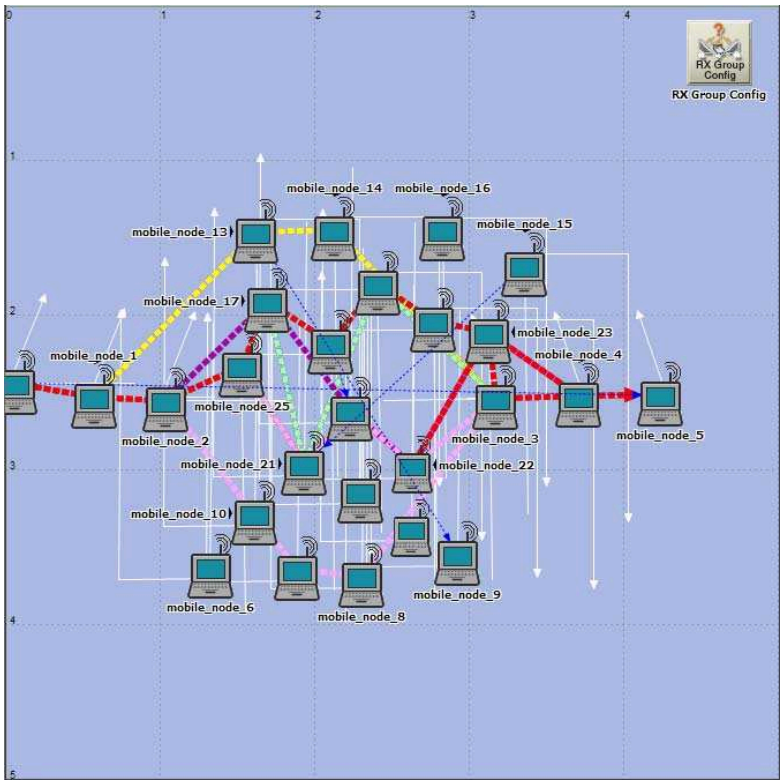
5.4.3 SMĚROVÁNÍ DAT

Pro zobrazení, jakou cestou probíhalo směrování dat, se zvolí z hlavní nabídky *Protocols → IP → Demands → Display Routes for Configured Demands.* V levém panelu okna lze vybrat cesty pro konkrétní požadavky. Pro přehlednost byl vybrán pouze jeden požadavek (*mobile_node_0 → mobile_node_5*). V pravé části okna lze vybrat a zobrazit cesty pro daný požadavek v určitém čase, což je znázorněno na obrázku 5.10 různými barvami. Lze si také všimnout, že jednotlivé stanice nejsou ve výchozí poloze vzhledem ke vzorovému modelu sítě, ale je zde využito funkce offsetu (zatrženo pole *Show node movement time offset*) pro znázornění polohy stanic v daném čase vzhledem ke zvolené trajektorii.



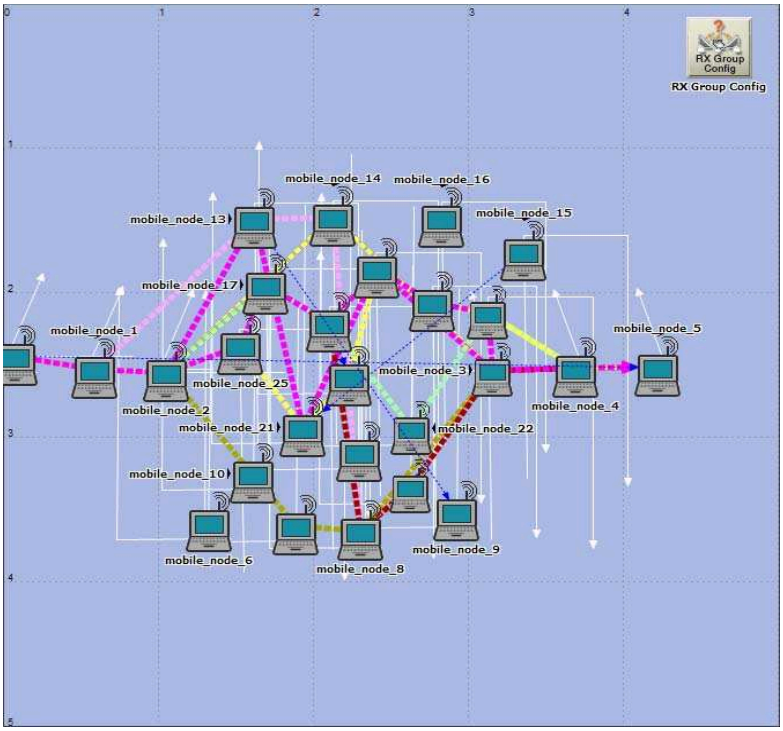
Obrázek 5.10 Směrování dat v AODV

Na obrázku 5.11 je uvedena ukázka směrování dat u protokolu OLSR. Při pohledu na obrázek se může zdát, že by směrování dat mohlo probíhat kratší cestou, ale je to správně. Musíme totiž brát na vědomí vlastnost protokolu OLSR a sice, že komunikuje s ostatními uzlu pouze přes své MPR a také neopomenout vzájemnou mobilitu uzlů.



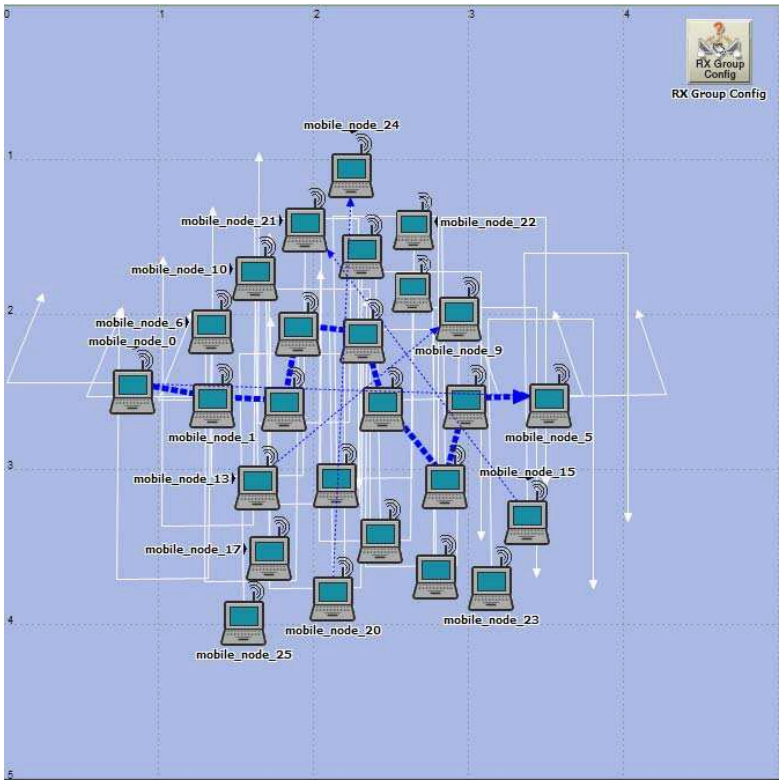
Obrázek 5.11 Směrování dat v OLSR

Směrování dat u protokolu DSR ukazuje obrázek 5.12. U tohoto protokolu dovoluje OM exportovat směrovací tabulku, která je pro požadavek (*mobile_node_0* → *mobile_node_5*) uvedena v příloze 2.



Obrázek 5.12 Směrování dat v DSR

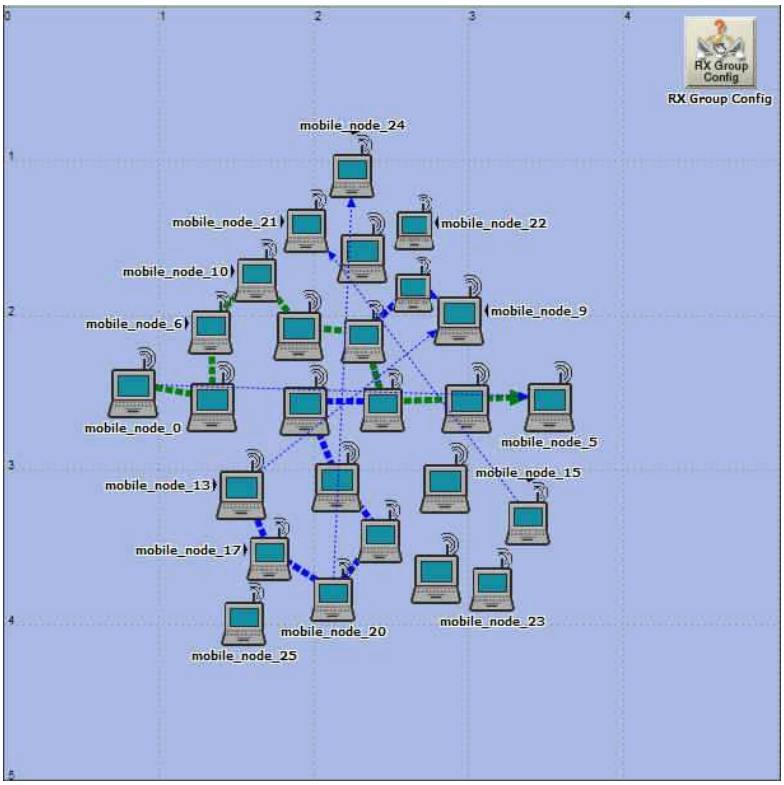
U protokolu TORA nenabízí OM zobrazení směrování dat v různých časech, ale pouze v jednom čase. Směrování dat je vidět na obrázku 5.13.



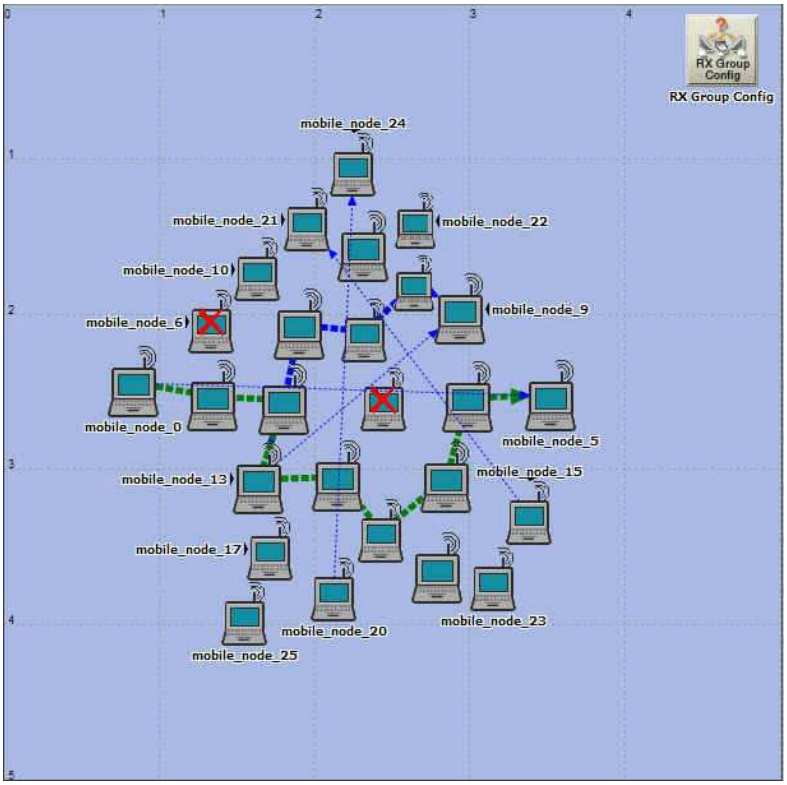
Obrázek 5.13 Směrování dat v TORA

Výpadek několika uzlů

Na posledním pátém simulovaném scénáři je ilustrována schopnost nalezení alternativní cesty v případě výpadku několika uzlu. Na obrázku 5.14 jsou ukázány původní cesty požadavků (*mobile_node_0* → *mobile_node_5* a *mobile_node_13* → *mobile_node_9*). A na obrázku 5.15 alternativní cesty těchto požadavků v případě výpadku dvou uzlů (červený křížek). Výpadek uzlu může například nastat v případě vypršení (expirace) spojení, nebo při vzdálení mobilního uzlu mimo dosah daného uzlu atd.



Obrázek 5.14 Původní cesty požadavků

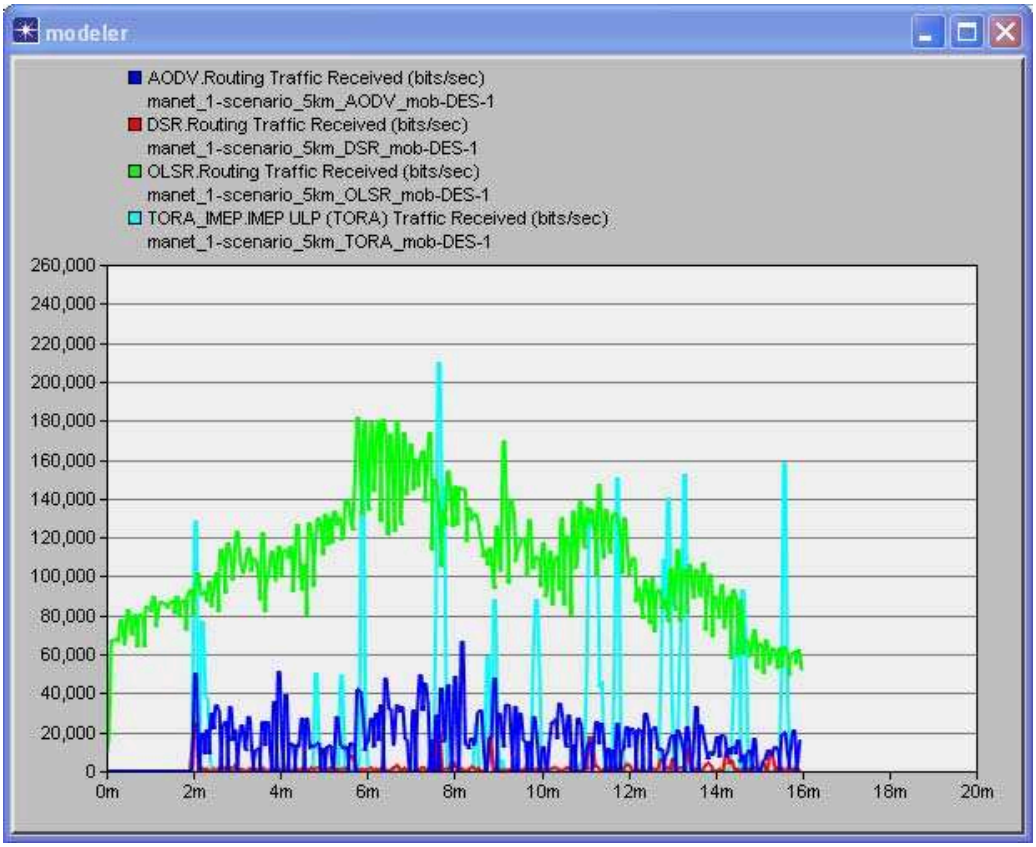


Obrázek 5.15 Alternativní cesty požadavků

5.4.4 POROVNÁNÍ SMĚROVACÍCH PROTOKOLŮ

K porovnání směrovacích protokolů poslouží statistiky vzniklé simulací jednotlivých protokolů současně. Směrovací protokoly budou porovnány jednak z pohledu množství směrovacích informací potřebných k nalezení cesty od zdroje k cíli a také z pohledu koncového zpoždění a kolísání zpoždění pro jednotlivé požadavky.

Na obrázku 5.16 je statistika množství přijatých směrovacích informací v bitech/s pro celou síť. Již na první pohled si lze všimnout rozdílu mezi proaktivním a reaktivním přístupem ke směrování. Zástupcem proaktivního přístupu je protokol OLSR (zelená křivka), kdy je zřejmé, že si protokol sestavuje směrovací tabulku již od počátku a v případě vzniku požadavku je cesta již známa, z čehož plyne nízké zpoždění. Na druhou stranu musí být tabulka při každé změně v síti aktualizována, což má za následek vysoké směrovací informace, které mohou vést až k zahlcení sítě. Zástupci reaktivního přístupu jsou protokoly AODV (modrá křivka) a DSR (červená křivka). Tyto protokoly začínají hledat cestu k cílovému uzlu až při vzniku požadavku, tedy okolo druhé minuty.

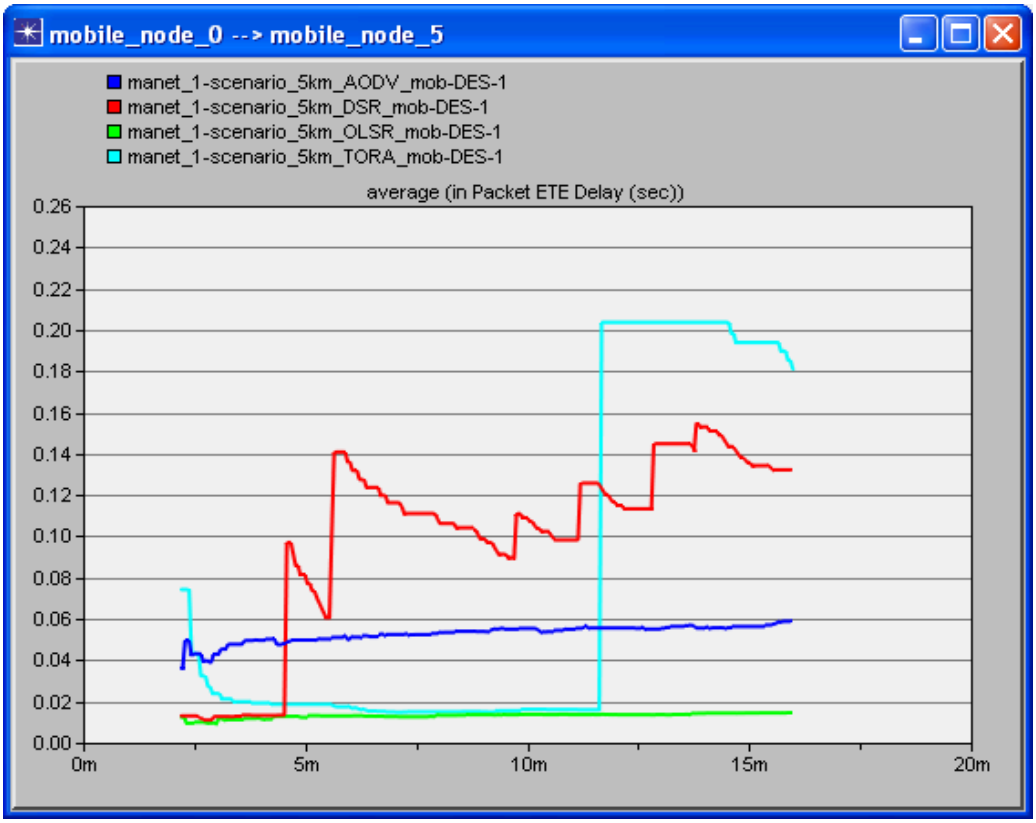


Obrázek 5.16 Množství přijatých směrovacích informací

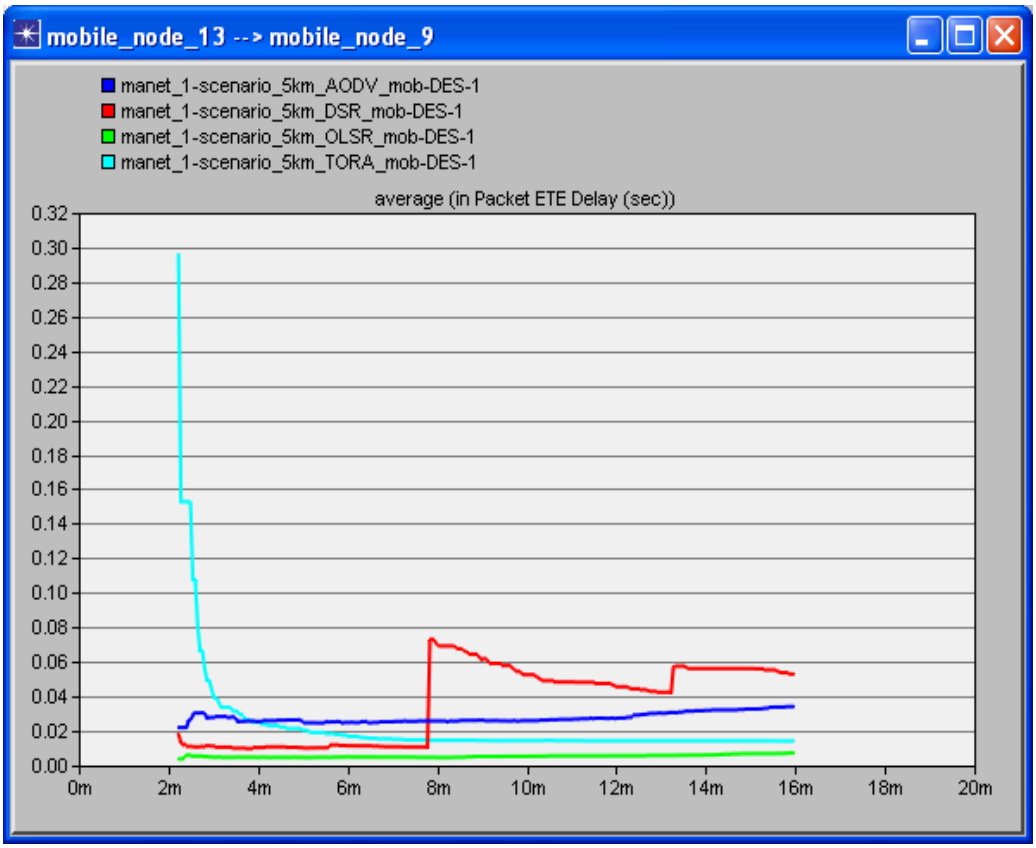
Protokol DSR nemá potřebu pravidelně zaplavovat síť aktualizací směrovacích tabulek, jako směrovací protokoly řízené tabulkou. Mezilehlé uzly jsou schopny efektivně využívat informace z paměti a tím redukovat režie, proto také protokol vykazuje nejnižší směrovací informace. Směrovací informace protokolu AODV jsou podstatně vyšší než-li u protokolu DSR, protože AODV používá periodické zasílání *HELLO* paketů pro zjištění informací o svých sousedních uzlech.

Protokol TORA (světle modrá křivka) využívá kombinaci proaktivního a reaktivního přístupu ke směrování, což má za následek špičky ve statistice.

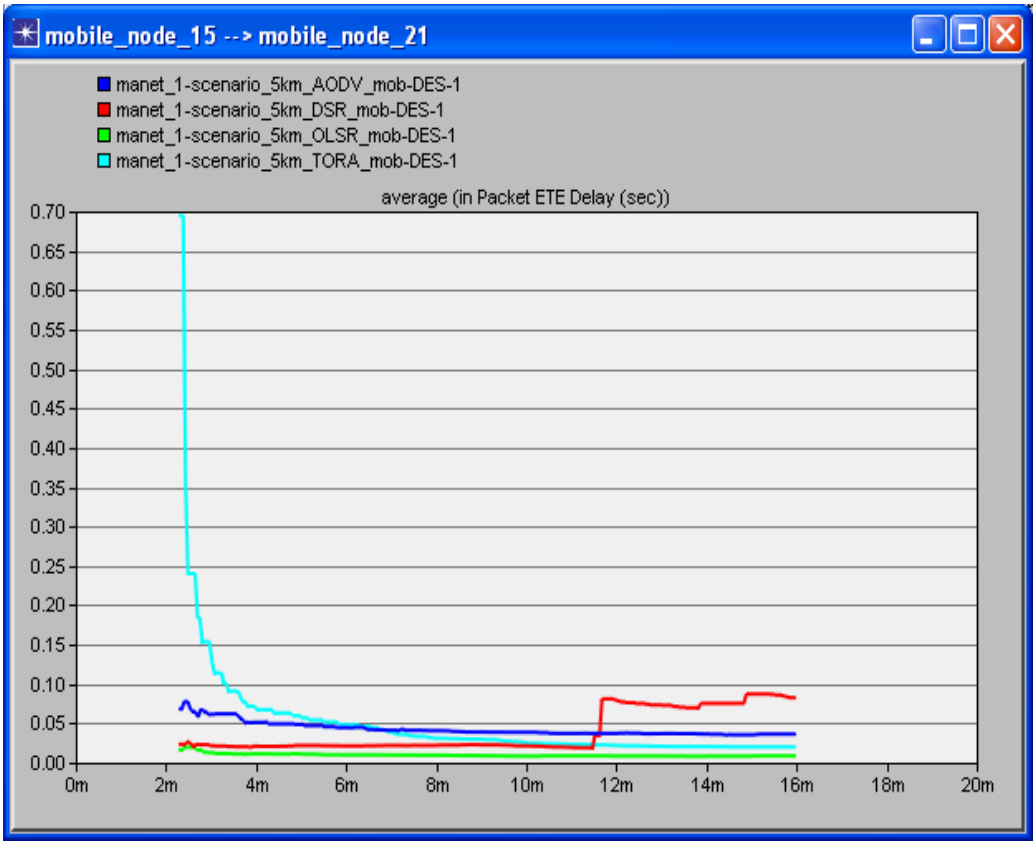
Na obrázcích 5.17-5.20 je znázorněno zpoždění pro jednotlivé požadavky provozu při použití jednotlivých směrovacích protokolů. Dle tabulky 3.2 maximální zpoždění nesmí přesáhnout 200 ms pro úspěšný přenos hlasu a videa. Této podmínce vyhovují pro všechny požadavky provozu protokoly OLSR, AODV a DSR, přičemž nejmenšího zpoždění dosahuje protokol OLSR, který již před vznikem požadavků zná cesty k jednotlivým uzlům. U protokolu DSR si můžeme všimnout výkyvů ve zpoždění, tyto výkyvy jsou způsobeny tím, že v určitý moment dojde ke ztrátě cesty a musí být znovu zahájeno hledání nové cesty, což způsobí prudký nárůst zpoždění, a po nalezení nové cesty dochází k jeho poklesu. Ke ztrátě cesty nejčastěji dochází vlivem mobility uzlů. U protokolu TORA jsou při vzniku požadavků, na začátku komunikace špičkové hodnoty, které jsou nejvíce vidět na obrázcích 5.18-5.20. Vzhledem k tomu, že se jedná o špičkové hodnoty na počátku komunikace, jsou způsobeny počátečním zjišťováním stavu okolí uzlu.



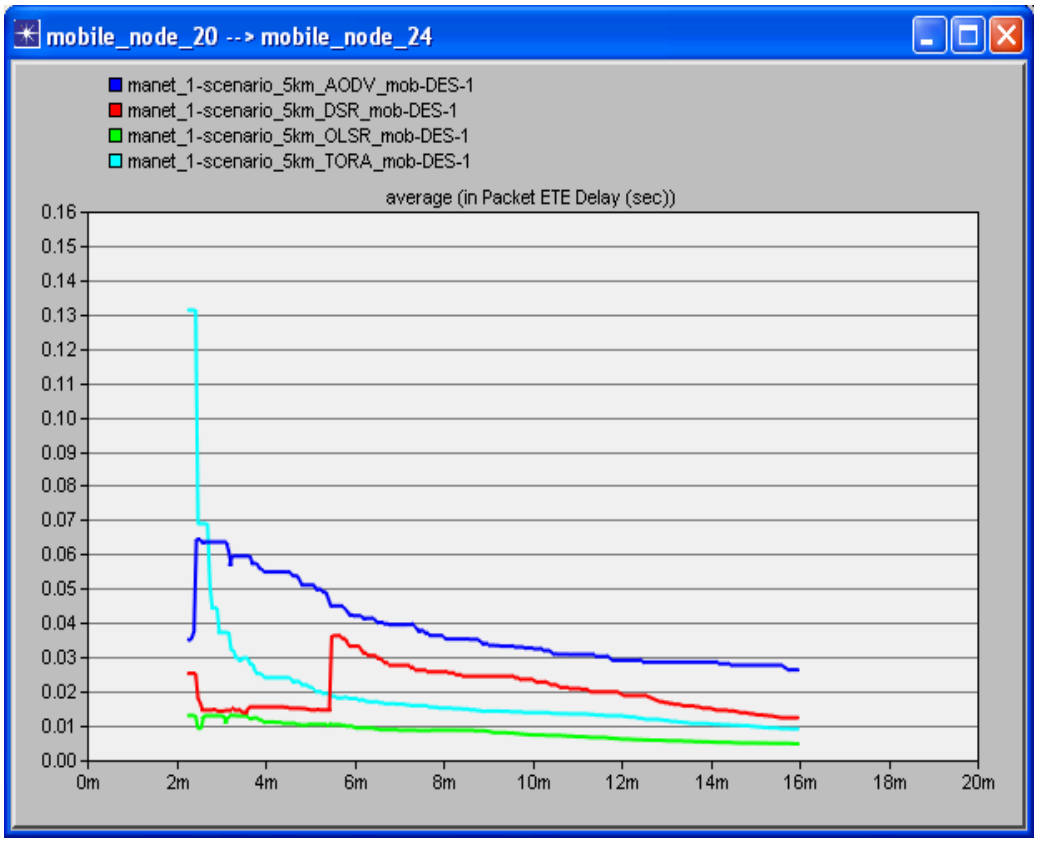
Obrázek 5.17 Zpoždění mobile_node_0 → mobile_node_5



Obrázek 5.18 Zpoždění mobile_node_13 → mobile_node_9

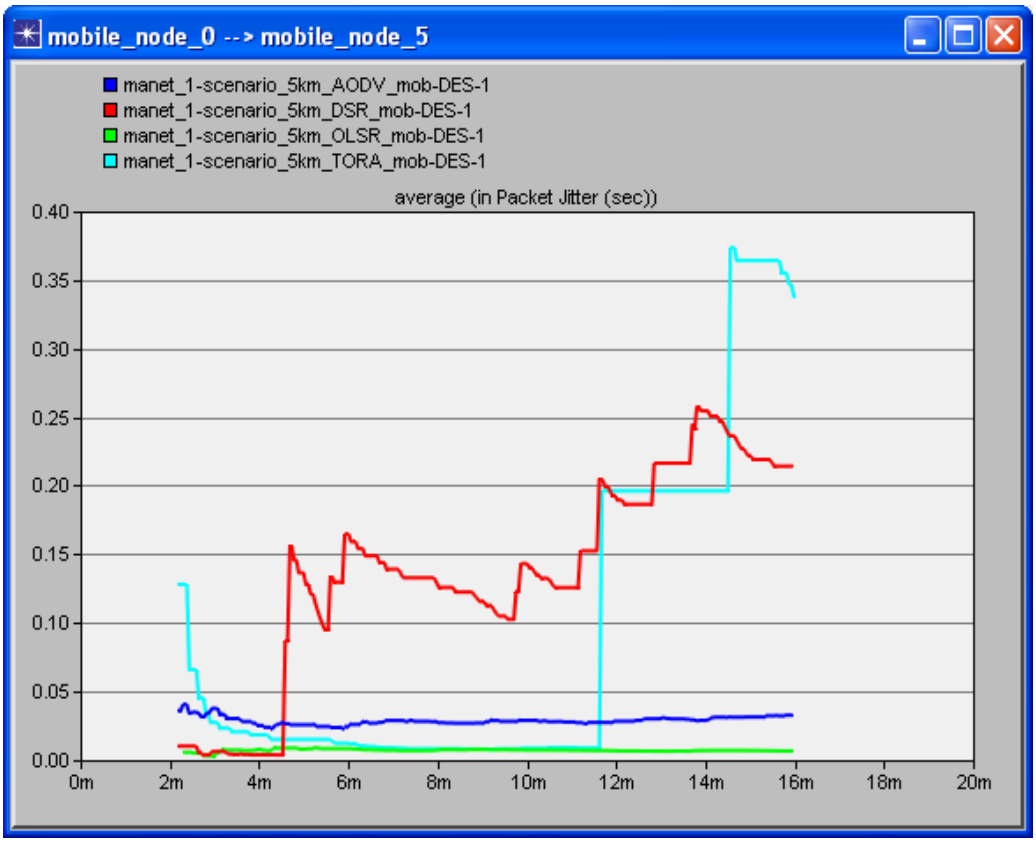


Obrázek 5.19 Zpoždění mobile_node_15 → mobile_node_21

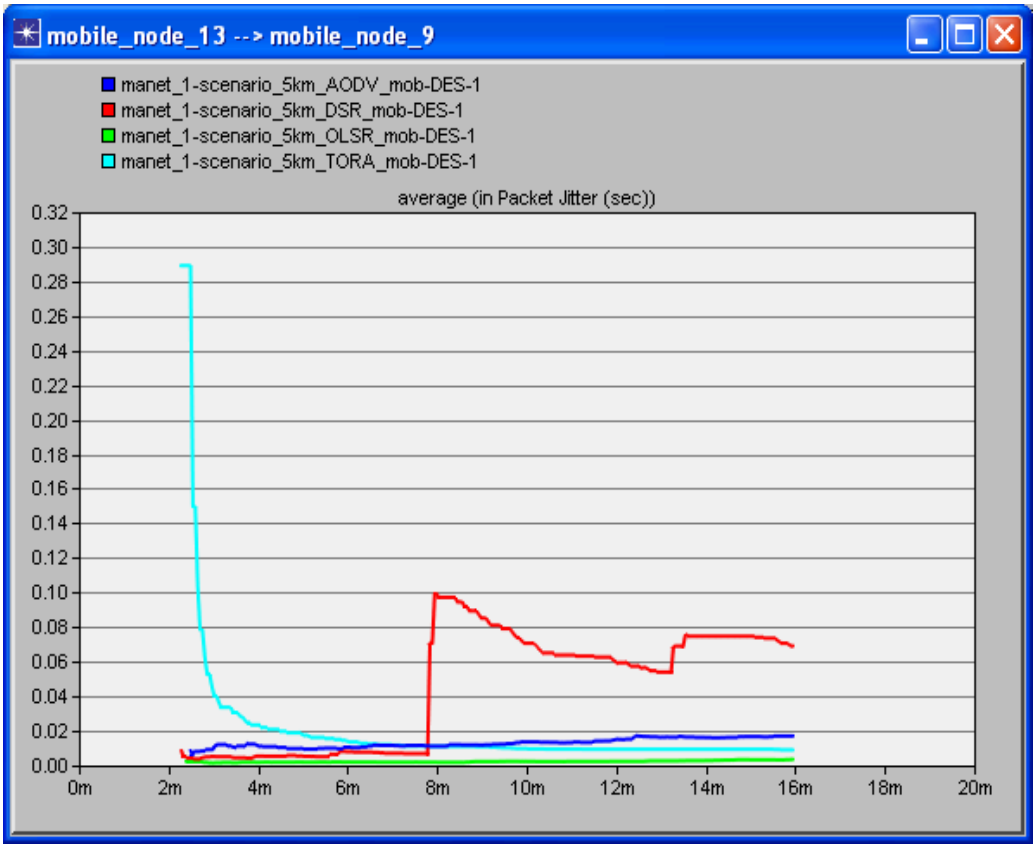


Obrázek 5.20 Zpoždění mobile_node_20 → mobile_node_24

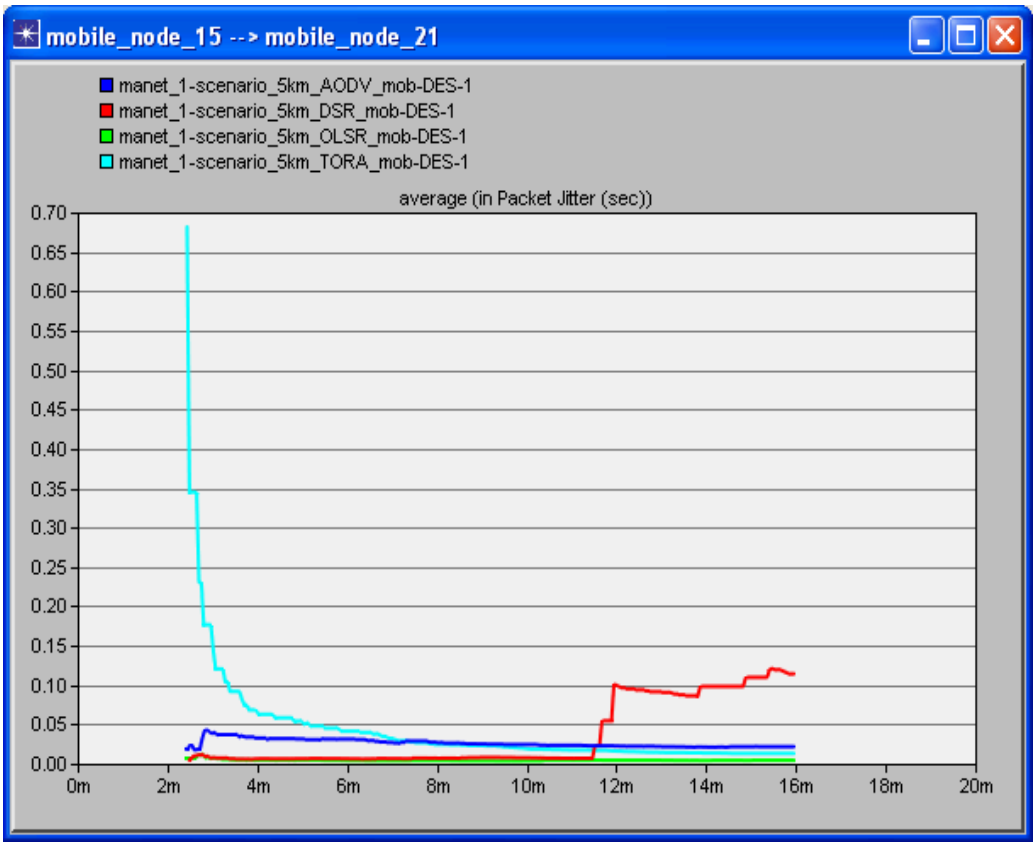
Při přenosu hlasu a videa přes síť je také důležitým parametrem kolísání zpoždění, neboli *jitter*. Jedná se o nejhoršího nepřítele hlasových služeb. Kolísání zpoždění v síti je variace v intervalech mezi příchody paketů, způsobené zátěží sítě, změnou topologie a směrováním v síti [1]. Podle tabulky 3.2 je maximální přípustné kolísání zpoždění 30 ms. Obrázky 5.21-5.24 ukazují jitter pro jednotlivé požadavky provozu a jednotlivé směrovací protokoly. Podobně jako u zpoždění i u kolísání vykazuje nejlepší výsledky protokol OLSR a splňuje podmínku 30 ms pro všechny požadavky provozu. Kolem hranice 30 ms se pohybují i výsledky protokolu AODV a pomineme-li špičkové hodnoty na počátku komunikace, tak i protokol TORA. Důvod špiček na počátku komunikace je stejný jako u zpoždění. Protokol DSR vykazuje podobně jako u zpoždění časté prudké výkyvy, způsobené opět ztrátou cest a mobilitou uzlů. Stejný původ mají také výkyvy u protokolu TORA (obrázek 5.21) a protokolu AODV (obrázek 5.24).



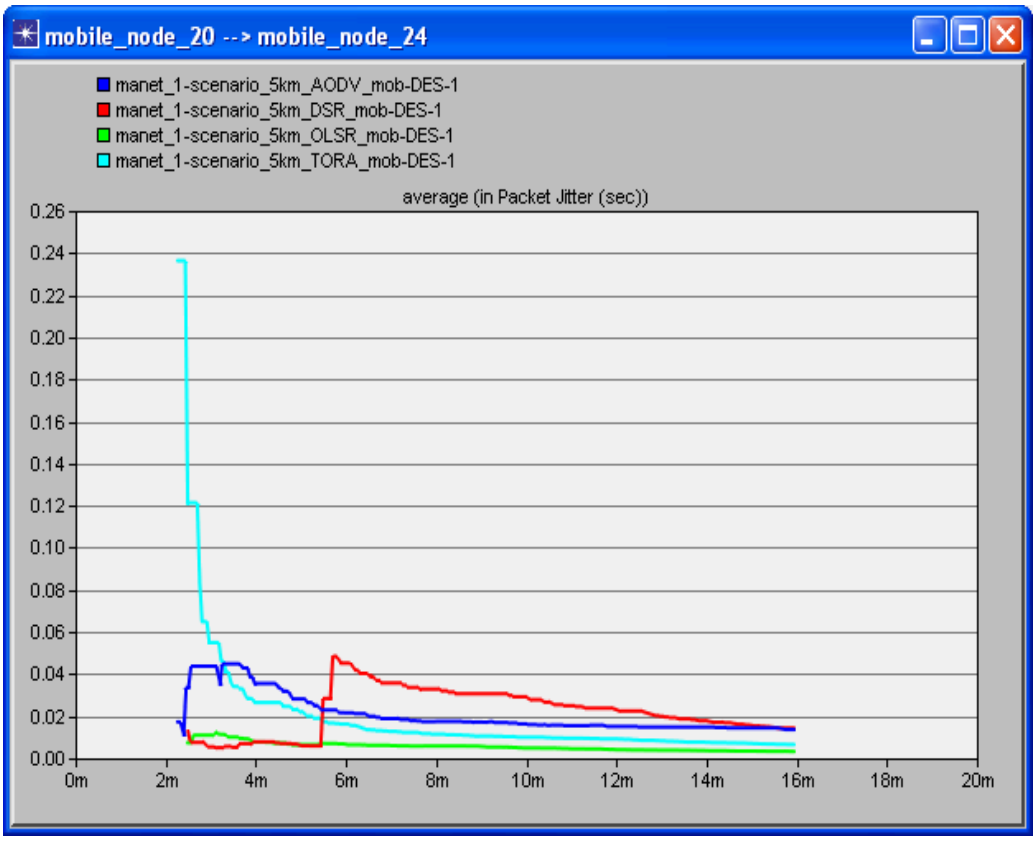
Obrázek 5.21 Jitter mobile_node_0 → mobile_node_5



Obrázek 5.22 Jitter mobile_node_13 → mobile_node_9



Obrázek 5.23 Jitter mobile_node_15 → mobile_node_21



Obrázek 5.24 Jitter mobile_node_20 → mobile_node_24

ZÁVĚR

Diplomová práce se zabývala směrovacími protokoly pro sítě s volnou topologií.

Mezi hlavní rysy bezdrátových Ad hoc sítí patří dynamická povaha sítě (časté změny topologie), dále síť postrádá pevnou infrastrukturu a každý uzel v síti může zastávat funkci směrovače a předávat tak data dalším uzlům. To je také hlavní rozdíl oproti drátovým síťovým technologiím. Všechny uzly v síti sdílejí přenosové médium, z čehož vyplývá náchylnost sítě k rušení. Mezi bezdrátové Ad hoc sítě patří senzorové sítě a mobilní Ad hoc sítě (MANET).

Uzly uvnitř MANET sítě (RFC 2501) se sami-organizují, mohou se volně pohybovat a tím rychle a nepředvídatelně měnit topologii sítě. Důležité je poznamenat, že MANET síť může vystupovat jak samostatně, tak může být i připojena do internetu. Topologie sítě mesh je charakteristická tím, že nabízí více možných spojů mezi uzly, kdy se může jednat o plně propojenou síť (*full mesh*), nebo o částečně propojenou síť (*partial mesh*). Sítě s takovou topologií jsou vysoce spolehlivé, ovšem za cenu velkých nákladů

Motorola MESH sítě jsou založeny na architektuře označované jako MEA (*Motorola Enable Access*), kdy každá koncová stanice současně funguje jako základnová. Je důležité říci, že taková mesh síť není novým typem rádiové modulace, jedná se pouze o spojení nynějších a nových rádiových technologií, což znamená, že tato technologie může být uplatněna na každé z rádiových schémat. MEA je prakticky schopna využívat spektrum od 900 MHz až po zhruba 7 GHz. Motorola MESH sítě v praxi poskytují tři řešení, a sice MOTOMESH Solo, MOTOMESH Duo a MOTOMESH Quattro. Solo řešení využívá jediné pásmo 2,4 GHz. Duo řešení je dostupné buď v konfiguraci s využitím pásma 2,4 GHz (802.11 b/g) nebo v konfiguraci s dodatečným pásmem 5,8; 5,4 nebo 4,9 GHz (802.11a). Poslední řešení Quattro využívá nelicencované pásmo 4,9 GHz a licencované pásmo 2,4 GHz a každý přístupový bod obsahuje dva WiFi a dva MEA standarty, což poskytuje flexibilní širokopásmový přístup.

V dnešních sítích se používají dva hlavní způsoby zajištění QoS a sice IntServ *(Integrated Services)* a DiffServ *(Differentiated Services).* Zajištění QoS v MANET je ovšem dosti složité, a to z důvodu časté změny topologie, spojovacích omezení a omezené šířky pásma. Mnoho návrhů řešení QoS pro internet nejsou vhodná pro použití v MANET, musí být přizpůsobena. Model IntServ ve spojitosti s RSVP není vhodný pro použití v MANET, protože by kladl obrovské nároky na paměť a zpracování režijních informací pro každý mobilní uzel. Model DiffServ také nelze použít, z důvodu nemožnosti přesně říci co je jádro (*core*) a vstupní nebo výstupní router. Proto v roce 2000 byl navržen model FQMM (*Flexible QoS Model for MANET*), který využívá jak vlastností IntServ, tak i vlastností DiffServ.

Směrovací protokoly v sítích s volnou topologií lze rozdělit do několika skupin. Protokoly popsány v DP patří do skupin proaktivních (OLSR) a reaktivních (AODV, DSR) protokolů. Proaktivní protokoly udržují trvale kompletní směrovací informace, které jsou pak ihned k dispozici, z čehož plyne nízké zpoždění. Na druhé straně reaktivní protokoly hledají cestu až v okamžiku vzniku požadavku, což má za následek zase větší zpoždění. Posledním uváděným protokolem je protokol TORA, který je jakousi směsí proaktivního a reaktivního směrování.

K určení, který protokol vykazoval nejlepší výsledky bylo potřeba protokoly důkladně porovnat. Vzhledem k tomu, že uzly sdílejí šířku pásma a šířka pásma je omezená je z tohoto pohledu důležitým faktorem množství směrovacích informací potřebných k nalezení cesty. Nejhorší výsledky vykazuje protokol OLSR, což se z podstaty proaktivního směrování dalo očekávat. Naopak výsledky nejlepší vykazuje protokol DSR, který nemá potřebu zaplavovat síť aktualizacemi směrovacích tabulek a cestu hledá jen na požádání. Abychom mohli říci, který protokol je nejlepší pro přenos dat citlivých na zpoždění a kolísání zpoždění (hlas, video) musíme protokoly porovnat i z těchto dvou pohledů. Hodnoty zpoždění a kolísání zpoždění jsou srovnávány s tabulkovými hodnotami, které jsou pro zpoždění 200 ms a pro kolísání 30 ms. Nejlepší protokol z pohledu zpoždění i kolísání zpoždění (jitter) je OLSR, dále také protokol AODV vykazuje velmi dobré výsledky. Nevýhoda protokolu DSR je ta, že nedokáže opravit rozbitou cestu, což způsobuje značné výkyvy jak zpoždění, tak kolísání zpoždění. Protokol TORA mimo počáteční špičkové hodnoty vykazuje taktéž velmi uspokojivé výsledky.

Směrovací protokoly v MANET vhodné pro přenos multimediálních dat (hlas, video) jsou protokoly OLSR a AODV. Pro model sítě vytvořený v rámci simulace je v poměru množství režijních informací/zpoždění resp. jitter nejlepší protokol AODV. Nelze však říci obecně, který z protokolů je nejlepší, je třeba vždy přihlédnout na danou topologii sítě, na množství uzlů, na počet a rychlost mobilních uzlů a také na dostupné zdrojové prostředky.

SEZNAM POUŽITÉ LITERATURY

[1] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 1. vyd. České Budějovice : KOPP, 2004. ISBN 80-7232-236-2. s. 275-276.

[2] CHAKRABARTI, Satyabrata, MISHRA, Amitabh. QoS Issues in Ad Hoc Wireless Networks. *IEEE Communications.*

[3] *Motorola Mesh Networks Technology Position Paper* [online]. 2004 [cit. 2007-11-20]. Dostupný z WWW: <http://www.motorola.com/mesh/pdf/wp_technology_position_paper.pdf>.

[4] MOLNÁR, Karol. *Zajištění QoS*. [s.l.] : [s.n.], [2006?]. 25 s. Dostupný z WWW: <http://www.utko.feec.vutbr.cz/~molnar/index.php?stranka=mmos>.

[5] MOLNÁR , Karol, ZEMAN, Otto. *Moderní síťové technologie laboratorní cvičení,*. Brno : VUT v Brně, Fakulta elektrotechniky, Ústav telekomunikací, 20 06. 91 s. Dostupný z WWW: <http://www.utko.feec.vutbr.cz/~molnar/MMOS/MMOS_lab.pdf>.

[6] BASAGNI, Stefano, et al. *Mobile Ad Hoc Networking : Kapitola 1.4.8. Quality of Service and Optimization*. [s.l.] : Wiley-IEEE, 2004. 480 s. ISBN 0471373133.

[7] CHEN, Lei, WENDI B., Heinzelman. A Survey of Routing Protocols that Support QoS in Mobile Ad Hoc Networks. *IEEE Network : The Magazine of Global Internetworking*. 2007, vol. 21, no. 6, s. 30-38.

[8] LUKE , Klein-Berndt. A Quick Guide to AODV Routing. *National Institute of Standards and Technology* [online]. 2006 [cit. 2008-03-15]. Dostupný z WWW: <http://w3.antd.nist.gov/wctg/aodv_kernel/aodv_guide.pdf>.

[9] *The Dynamic Source Routing Protocol (DSR) : RFC 4728* [online]. 2007 [cit. 2008-03-18]. Dostupný z WWW: <http://tools.ietf.org/html/rfc4728#section-3.1>.

[10] *Temporally-Ordered Routing Algorithm (TORA) Functional Specification : Internet draft* [online]. 2001 [cit. 2008-03-19]. Dostupný z WWW: <http://tools.ietf.org/html/draft-ietf-manet-tora-spec-04>.

[11] *Optimized Link State Routing Protocol (OLSR) : RFC 3626* [online]. 2003 [cit. 2008-03-25]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc3626.txt>.

[12] *Quality of Service for Ad hoc Optimized Link State Routing Protocol (QOLSR)* : Internet draft [online]. 2007 [cit. 2008-03-26]. Dostupný z WWW: <http://www3.tools.ietf.org/html/draft-badis-manet-qolsr-05>.

[13] *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations :* RFC 2501 [online]. 1999 [cit. 2008-02-20]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc2501.txt>.

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha 1: Ukázka části textového souboru manet_1 – scenario_5km_AODV_mob-DES-1-conv_flow_routes.gdf

```
Campus Network.mobile_node_0,Campus
Network.mobile_node_5,131.65,0,mobile_node_0 --> mobile_node_5,Campus
Network.mobile_node_0,None,Campus Network.mobile_node_1,None,Campus
Network.mobile_node_13,None,Campus Network.mobile_node_14,None,Campus
Network.mobile_node_3,None,Campus Network.mobile_node_4,None

Campus Network.mobile_node_0,Campus
Network.mobile_node_5,131.65,1,mobile_node_0 --> mobile_node_5,Campus
Network.mobile_node_0,None,Campus Network.mobile_node_1,None,Campus
Network.mobile_node_13,None,Campus Network.mobile_node_14,None,Campus
Network.mobile_node_3,None,Campus Network.mobile_node_4,None

Campus Network.mobile_node_13,Campus
Network.mobile_node_9,131.95,2,mobile_node_13 --> mobile_node_9,Campus
Network.mobile_node_13,None,Campus Network.mobile_node_14,None,Campus
Network.mobile_node_3,None

Campus Network.mobile_node_13,Campus
Network.mobile_node_9,131.96,3,mobile_node_13 --> mobile_node_9,Campus
Network.mobile_node_13,None,Campus Network.mobile_node_14,None,Campus
Network.mobile_node_3,None

Campus Network.mobile_node_0,Campus
Network.mobile_node_5,132.48,4,mobile_node_0 --> mobile_node_5,Campus
Network.mobile_node_0,None,Campus Network.mobile_node_1,None,Campus
Network.mobile_node_13,None,Campus Network.mobile_node_14,None,Campus
Network.mobile_node_3,None,Campus Network.mobile_node_4,None

Campus Network.mobile_node_20,Campus
Network.mobile_node_24,135.97,5,mobile_node_20 -->
mobile_node_24,Campus Network.mobile_node_20,None,Campus
Network.mobile_node_18,None,Campus Network.mobile_node_14,None,Campus
Network.mobile_node_8,None,Campus Network.mobile_node_11,None

Campus Network.mobile_node_20,Campus
Network.mobile_node_24,135.98,6,mobile_node_20 -->
mobile_node_24,Campus Network.mobile_node_20,None,Campus
Network.mobile_node_18,None,Campus Network.mobile_node_14,None,Campus
Network.mobile_node_8,None,Campus Network.mobile_node_11,None
```

Příloha 2: Směrovací tabulka protokolu DSR

DSR.DSR Routes Report

File Edit View Help

	Time	Source Node Name	Destination Node Name	Hop Count	
41	131.673046	192.0.0.1 (Campus Network.mobile_node_0)	192.0.0.6 (Campus Network.mobile_node_5)	6	192.0.0.1 (Campus Network.mobile_node_0)
42					192.0.0.2 (Campus Network.mobile_node_1)
43					192.0.0.3 (Campus Network.mobile_node_2)
44					192.0.0.15 (Campus Network.mobile_node_14)
45					192.0.0.4 (Campus Network.mobile_node_3)
46					192.0.0.5 (Campus Network.mobile_node_4)
47					192.0.0.6 (Campus Network.mobile_node_5)
48					
49	131.920726	192.0.0.1 (Campus Network.mobile_node_0)	192.0.0.6 (Campus Network.mobile_node_5)	6	192.0.0.1 (Campus Network.mobile_node_0)
50					192.0.0.2 (Campus Network.mobile_node_1)
51					192.0.0.3 (Campus Network.mobile_node_2)
52					192.0.0.15 (Campus Network.mobile_node_14)
53					192.0.0.4 (Campus Network.mobile_node_3)
54					192.0.0.5 (Campus Network.mobile_node_4)
55					192.0.0.6 (Campus Network.mobile_node_5)
56					
57	131.954423	192.0.0.14 (Campus Network.mobile_node_13)	192.0.0.10 (Campus Network.mobile_node_9)	4	192.0.0.14 (Campus Network.mobile_node_13)
58					192.0.0.15 (Campus Network.mobile_node_14)
59					192.0.0.4 (Campus Network.mobile_node_3)
60					192.0.0.13 (Campus Network.mobile_node_12)
61					192.0.0.10 (Campus Network.mobile_node_9)
62					
63	131.967737	192.0.0.14 (Campus Network.mobile_node_13)	192.0.0.10 (Campus Network.mobile_node_9)	4	192.0.0.14 (Campus Network.mobile_node_13)
64					192.0.0.15 (Campus Network.mobile_node_14)
65					192.0.0.4 (Campus Network.mobile_node_3)
66					192.0.0.13 (Campus Network.mobile_node_12)
67					192.0.0.10 (Campus Network.mobile_node_9)
68					
69	132.051404	192.0.0.1 (Campus Network.mobile_node_0)	192.0.0.6 (Campus Network.mobile_node_5)	6	192.0.0.1 (Campus Network.mobile_node_0)
70					192.0.0.2 (Campus Network.mobile_node_1)
71					192.0.0.3 (Campus Network.mobile_node_2)
72					192.0.0.15 (Campus Network.mobile_node_14)
73					192.0.0.4 (Campus Network.mobile_node_3)
74					192.0.0.5 (Campus Network.mobile_node_4)
75					192.0.0.6 (Campus Network.mobile_node_5)
76					
77	135.920532	192.0.0.14 (Campus Network.mobile_node_13)	192.0.0.10 (Campus Network.mobile_node_9)	4	192.0.0.14 (Campus Network.mobile_node_13)
78					192.0.0.15 (Campus Network.mobile_node_14)
79					192.0.0.4 (Campus Network.mobile_node_3)
80					192.0.0.13 (Campus Network.mobile_node_12)
81					192.0.0.10 (Campus Network.mobile_node_9)
82					
83	135.982821	192.0.0.21 (Campus Network.mobile_node_20)	192.0.0.25 (Campus Network.mobile_node_24)	6	192.0.0.21 (Campus Network.mobile_node_20)
84					192.0.0.19 (Campus Network.mobile_node_18)
85					192.0.0.15 (Campus Network.mobile_node_14)
86					192.0.0.4 (Campus Network.mobile_node_3)
87					192.0.0.13 (Campus Network.mobile_node_12)
88					192.0.0.12 (Campus Network.mobile_node_11)
89					192.0.0.25 (Campus Network.mobile_node_24)
90					
91	135.999870	192.0.0.21 (Campus Network.mobile_node_20)	192.0.0.25 (Campus Network.mobile_node_24)	6	192.0.0.21 (Campus Network.mobile_node_20)
92					192.0.0.19 (Campus Network.mobile_node_18)