

مقایسه پروتکل های مسیریابی

AODV, DSR, OLSR در شبکه های اقتصانی

متحرک (MANET) با نرم افزار شبیه سازی

OPNET

Performance Comparison for AODV,  
DSR, OLSR Routing in MANET  
Using OPNET Simulator

تهیه کننده:

صادق خیرالهی حسین آبادی

...

Sadegh.kheyrollahi@gmail.com

مجید خیرالهی حسین آبادی

دانشجوی کارشناسی ارشد مهندسی برق-مخابرات

Majid.kheyrollahi@gmail.com

حضرت علی (ع): ایمان آن است که راستی را برگزینی که به زیان تو بود بر دروغی که تو را سود دهد و گفتارت بر کردارت نیفزاید و چون از دیگری سخن گویی ترس از خدا در دلت آید.

هر چند از این نظام آموزشی، دل پری دارم و ناکفته های بسیار... در حال در این مقطع آموزش، از اساتید کرامتداری از جمله جناب آقایان دکتر جلالی، دکتر نصر، دکتر چراغی، دکتر نیک مهر، دکتر شادی نژاد، سرکار خانم علوی و استاد کرامتدور دکتر ناصر موحدی نیا بارها سپاسی های ارزشمندشان، کمال تشکر و قدردانی را دارم و از خداوند متعال آرزوی توفیق و سلامت را برایشان مسئلت دارم.

رندی و قلندری و عرفان بازی      عنوان جهالت است و هزریان بانی

بگذر ز نشان و نام و عنوان و لقب      کرده خدایه تو ضمیری صافی

## تقدیم به

ساحت مقدس یوسف زهرا (عج) که چشم ما برای زیارت صبحش بیدارند...

پدر و مادر عزیزم

آنان که از برکت وجودشان وجود یافتیم و در سایه سار محبتشان آرامش گرفتیم و اگر نبودند، نبود آنچه که

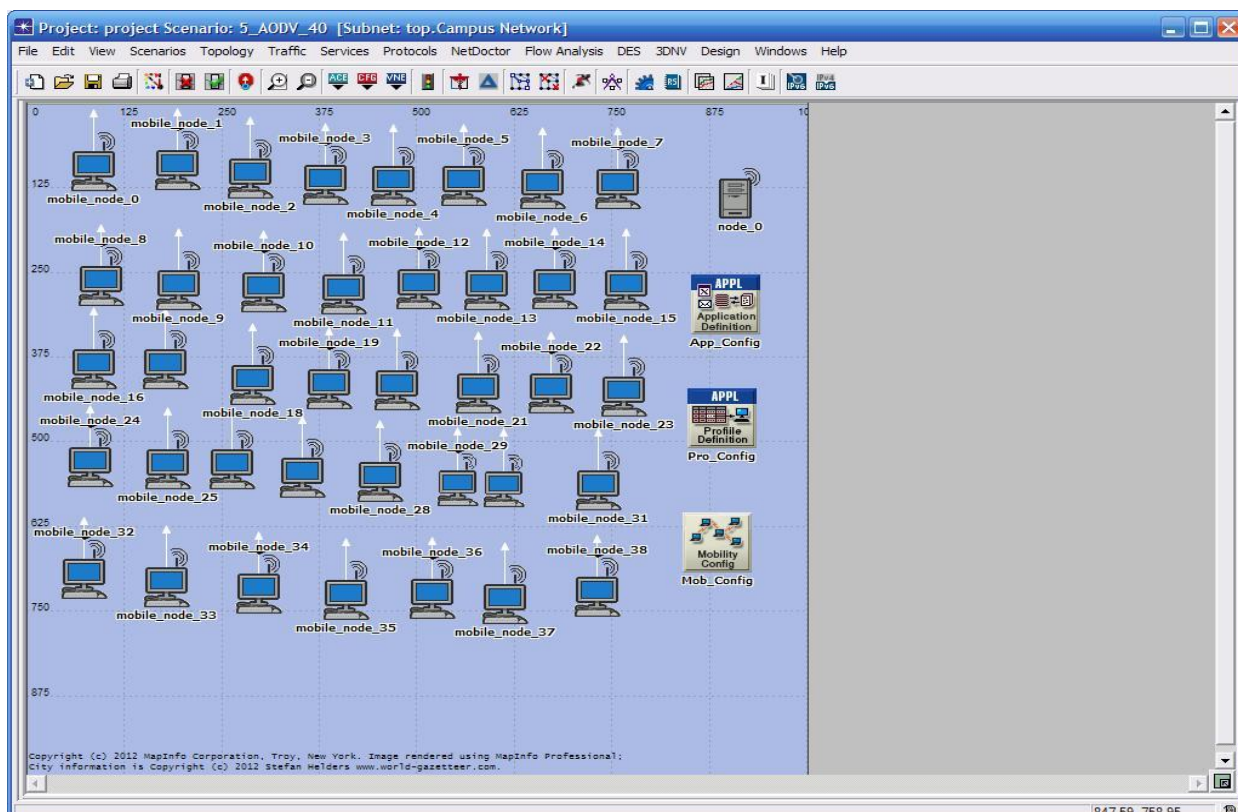
اکنون دارم و اگر هستم و ایستاده ام از هستی شان است.

عاشقان و رهروان طریق علم و معرفت



## چکیده

شبکه های اقتضائی شبکه هایی هستند که برای مسیریابی از هیچ عنصر کمکی شبکه ای استفاده نمی کنند ، بلکه در این شبکه ها خود گره های شرکت کننده در شبکه وظیفه مسیریابی شبکه را به عهده دارند. این شبکه ها شامل مجموعه ای از گره های توزیع شده اند که بدون پشتیبانی مدیریت مرکزی ، یک شبکه موقت را می سازند و با همدیگر به طور بی سیم ارتباط دارند . طبیعی ترین مزیت استفاده از این شبکه ها عدم نیاز به ساختار فیزیکی و امکان ایجاد تغییر در ساختار مجازی آنها است. مهم ترین ویژگی این شبکه ها وجود یک توپولوژی پویا و متغیر می باشد که نتیجه تحرک نودها می باشد. نودها در این شبکه ها به طور پیوسته موقعیت خود را تغییر می دهند که این خود نیاز به یک پروتکل مسیریابی که توانایی سازگاری با این تغیرات را داشته، نمایان می کند. این ویژگی های خاصی که دارند ، پروتکل های مسیریابی و روشهای امنیتی خاصی را می طلبد و از چالش های امروز این شبکه ها می باشد. تاکنون پروتکل های مسیریابی زیادی برای شبکه های اقتضائی پیشنهاد شده است. هدف از طراحی این پروتکل ها کمینه سازی یک یا چند عامل محدود کننده راندمان شبکه مثل محدودیت توان عملیاتی گره ها ، سربارهای کنترلی و سربارهای پردازشی است. شبیه سازها از لحاظ گوناگونی متعدد می باشند و هر کدام از آنها محاسن و معایبی را به همراه دارند که یکی از این شبیه سازهای معروف OPNET نام دارد . با توجه به اهمیت موضوع مسیریابی در شبکه های اقتضائی متحرک ، در این پایان نامه سه پروتکل متداول مسیریابی در محیط شبکه اقتضائی متحرک مقایسه شده و نتایج آن با پارامترهای میزان تاخیر ، میزان سربار ، بار شبکه و توان شبکه بدست آمده است . محیط شبکه اقتضائی شامل ۲۰ نود متحرک بوده و برای مقایسه پروتکل ها در مواجهه با تغییرات ، پنج محیط دیگر با نود های متحرک و شرایط مختلف نیز پیاده سازی شده و شبیه سازی بر روی آن اجرا گردیده است . در این شبیه سازی با شرایط و پارامترهای خاص آن ، درمجموع پروتکل OLSR عملکرد بهتری داشت ولی با توجه به شرایط و مقتضیات ، هر کدام از این پروتکل ها در جایگاه خود مورد بهره برداری قرار می گیرند و ممکن است در شرایط دیگری نتایج مختلفی بدست آید .



## فهرست مطالب

صفحه	عنوان
۱۶	فصل اول: پیشگفتار
۱۷	۱ + پیشگفتار
۱۸	فصل دوم : شبکه های اقتضائی متحرک
۱۹	۱-۲ مقدمه
۱۹	۲-۲ شبکه های بی سیم
۱۹	۳-۲ امنیت شبکه
۲۰	۴-۲ توپولوژی های شبکه بی سیم
۲۱	۱-۴-۲ مدل Infra Structure یا (Basic Service Set)
۲۱	۲-۴-۲ مدل ad-hoc
۲۳	۵-۲ شبکه های اقتضائی بی سیم
۲۴	۱-۵-۲ خصوصیات شبکه های اقتضائی
۲۴	۲-۵-۲ انواع شبکه های اقتضائی بی سیم
۲۵	۱-۲-۵-۲ شبکه های موردی (اقتضائی) سیار
۲۵	۲-۲-۵-۲ شبکه های حسگر بی سیم
۲۶	۳-۲-۵-۲ شبکه های توری بی سیم
۲۶	۶-۲ شبکه های اقتضائی متحرک
۲۶	۱-۶-۲ ساختار شبکه های اقتضائی متحرک
۲۸	۲-۶-۲ خصوصیات شبکه های اقتضائی متحرک
۳۰	۱-۲-۶-۲ مزایای شبکه های اقتضائی متحرک
۳۰	۳-۶-۲ معایب شبکه های اقتضائی متحرک
۳۲	۴-۶-۲ کاربردهای شبکه های اقتضائی متحرک
۳۴	۵-۶-۲ امنیت شبکه های اقتضائی متحرک
۳۵	۱-۵-۶-۲ انواع حملات بر روی شبکه های اقتضائی

۳۶	۲-۵-۶-۲	اهداف امنیتی در شبکه های اقتضائی متحرک
۳۸	۲-۵-۶-۳	چالش های امنیتی در شبکه های اقتضائی متحرک
۳۸	۷-۲	جمع بندی
۳۹		<b>فصل سوم : مسیریابی</b>
۴۰	۱-۳	مقدمه
۴۰	۲-۳	الگوریتم های مسیریابی
۴۱	۱-۲-۳	دیدگاه های الگوریتم های مسیریابی
۴۱	۱-۱-۲-۳	به صورت ایستا مسیریابی
۴۲	۲-۱-۲-۳	به صورت دینامیک یا پویا مسیریابی
۴۳	۳-۳	اصل بهینگی
۴۳	۴-۳	مسیر یابی کوتاه ترین مسیر
۴۴	۵-۳	الگوریتم غرق کردن ( سیل آسا )
۴۵	۶-۳	مسیر یابی بردار فاصله
۴۶	۷-۳	مسئله بی نهایت گرایی
۴۷	۸-۳	الگوریتم حالت لینک (پیوند)
۵۰	۹-۳	مسیریابی سلسله مراتبی
۵۰	۱۰-۳	مسیریابی فراگیر
۵۱	۱۱-۳	مسیریابی چند پخشی
۵۱	۱۲-۳	مسیریابی برای میزبان های سیار
۵۴	۱۳-۳	مسیریابی در شبکه های موقتی
۵۵	۱۴-۳	جمع بندی
۵۶		<b>فصل چهارم : مسیریابی شبکه های اقتضائی</b>
۵۷	۱-۴	مقدمه
۵۷	۲-۴	معیارهای طبقه بندی روش ها
۵۸	۱-۲-۴	از دیدگاه نوع ذخیره کردن اطلاعات مسیریابی
۵۸	۲-۲-۴	از لحاظ بروز رسانی
۵۹	۳-۲-۴	از لحاظ کنترل
۵۹	۴-۲-۴	از لحاظ نوع محاسبه مسیر
۶۰	۵-۲-۴	از لحاظ ساختار

۶۰	پروتکل های مسیریابی متداول در شبکه های اقتضائی	۳-۴
۶۱	پروتکل های تقسیم بندی اول	۱-۳-۴
۶۲	پروتکل های کنش گرا - فعال ( بر حسب جدول)	۱-۱-۳-۴
۶۲	پروتکل مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد DSDV	۱-۱-۱-۳-۴
۶۴	پروتکل مسیریابی بی سیم WRP	۲-۱-۱-۳-۴
۶۵	پروتکل مسیریابی تغییر وضعیت دروازه سرگروه (سردسته درگاه) CGSR	۳-۱-۱-۳-۴
۶۶	پروتکل مسیریابی تطبیقی درخت منبع STAR	۴-۱-۱-۳-۴
۶۶	مسیریابی حالت سلسله مراتبی HSR	۵-۱-۱-۳-۴
۶۸	پروتکل های واکنشی ( بر حسب تقاضا)	۲-۱-۳-۴
۶۸	پروتکل مسیریابی پایداری (ثبات) سیگنال SSR	۱-۲-۱-۳-۴
۶۸	پروتکل مسیریابی از مبداء پویا DSR	۲-۲-۱-۳-۴
۶۸	پروتکل مسیریابی منظم زمانی TORA	۳-۲-۱-۳-۴
۷۰	ایجاد مسیر	۱-۳-۲-۱-۳-۴
۷۱	نگهداری مسیر	۲-۳-۲-۱-۳-۴
۷۲	پاک کردن مسیر	۳-۳-۲-۱-۳-۴
۷۲	الگوریتم های مورد استفاده در TORA	۴-۳-۲-۱-۳-۴
۷۳	معایب پروتکل TORA	۵-۳-۲-۱-۳-۴
۷۳	خواص پروتکل TORA	۶-۳-۲-۱-۳-۴
۷۴	پروتکل مسیریابی مبتنی بر شرکت پذیری ABR	۴-۲-۱-۳-۴
۷۴	پروتکل مسیریابی بردار مسافت بر حسب تقاضا اقتضائی AODV	۵-۲-۱-۳-۴
۷۴	میکرو تفاوت (تنوع جزئی) مسیریابی فاصله نسبی RDMAR	۶-۲-۱-۳-۴
۷۴	پروتکل های ترکیبی - پیوندی ( بر حسب جدول و بر حسب تقاضا )	۳-۱-۳-۴
۷۵	پروتکل مسیریابی ناحیه ای ZRP	۱-۳-۱-۳-۴
۷۵	پروتکل های تقسیم بندی دوم	۲-۳-۴
۷۵	پروتکل های مسیریابی تخت ( مسطح )	۱-۲-۳-۴
۷۵	پروتکل های تخت فعال ( بر حسب جدول)	۱-۱-۲-۳-۴
۷۵	پروتکل های تخت واکنشی ( بر حسب تقاضا)	۲-۱-۲-۳-۴
۷۶	پروتکل های تخت ترکیبی	۳-۱-۲-۳-۴
۷۶	پروتکل های مسیریابی سلسله مراتبی	۲-۲-۳-۴
۷۶	پروتکل های مسیریابی مبتنی بر موقعیت جغرافیائی	۳-۲-۳-۴

۷۷	پروتکل مسیریابی از مبدا پویا	۴-۴
۷۷	کشف مسیر	۱-۴-۴
۷۷	نگهداری مسیر	۲-۴-۴
۸۰	اصول نگهداری مسیر در پروتکل مسیریابی از مبدا پویا	۳-۴-۴
۸۳	مزایای پروتکل مسیریابی از مبدا پویا	۴-۴-۴
۸۳	معایب پروتکل مسیریابی از مبدا پویا	۵-۴-۴
۸۳	یک مثال از پروتکل مسیریابی از مبدا پویا	۶-۴-۴
۸۵	پروتکل مسیریابی بردار مسافت بر حسب تقاضا اقتضائی	۵-۴
۸۷	کشف مسیر	۱-۵-۴
۸۹	ساخت و پخش بسته درخواست مسیر توسط گره مبدا	۱-۱-۵-۴
۹۱	نگهداری مسیر	۲-۵-۴
۹۲	مزایای پروتکل مسیریابی بردار مسافت بر حسب تقاضا	۳-۵-۴
۹۲	یک مثال از پروتکل مسیریابی بردار مسافت بر حسب تقاضا	۴-۵-۴
۹۴	پروتکل مسیریابی حالت پیوند بهینه	۶-۴
۹۶	انواع پیام ها	۱-۶-۴
۹۶	پیام سلام	۱-۱-۶-۴
۹۷	الگوریتم انتخاب نقاط ارسال چند نقطه ای	۱-۱-۱-۶-۴
۹۹	پیام کنترل توپولوژی	۲-۱-۶-۴
۱۰۰	جدول مسیریابی	۲-۶-۴
۱۰۰	خصوصیات پروتکل OLSR	۳-۶-۴
۱۰۰	جمع بندی	۷-۴
۱۰۲	<b>فصل پنجم : شبیه سازی</b>	
۱۰۳	مقدمه	۱-۵
۱۰۳	آشنایی با مفاهیم اولیه نرم افزار شبیه سازی (OPNET)	۲-۵
۱۰۴	پارامترهای ارزیابی	۳-۵
۱۰۴	میزان تاخیر	۱-۳-۵
۱۰۵	توان	۲-۳-۵
۱۰۵	میزان سربار	۳-۳-۵
۱۰۵	بار شبکه	۴-۳-۵
۱۰۵	فرآیند شبیه سازی	۴-۵



۱۰۶	اجرای نرم افزار OPNET و پیاده سازی شبیه سازی	۵-۵
۱۱۵	نتایج شبیه سازی	۶-۵
۱۱۵	نتایج پروتکل AODV در ۴ محیط	۱-۶-۵
۱۱۸	نتایج پروتکل DSR در ۴ محیط	۲-۶-۵
۱۲۱	نتایج پروتکل OLSR در ۴ محیط	۳-۶-۵
۱۲۴	نتایج ارزیابی محیط ها با مقایسه سه پروتکل	۴-۶-۵
۱۳۵	شبیه سازی دو محیط دیگر با ارائه نتایج	۵-۶-۵
۱۳۹	جمع بندی	۷-۵
۱۴۰	<b>فصل ششم : جمع بندی و ارائه پیشنهادات</b>	
۱۴۱	جمع بندی و ارائه پیشنهادات	۱-۶
۱۴۴	<b>پیوست الف آموزش نرم افزار شبیه سازی OPNET</b>	
۱۴۵	مقدمه	الف-۱
۱۴۵	کاربردهای مهم OPNET	الف-۲
۱۴۶	توصیف کاملی از شبیه ساز OPNET	الف-۳
۱۴۶	OPNET در مقایسه با سایر شبیه سازها	الف-۴
۱۴۷	نصب OPNET	الف-۵
۱۵۰	ساختار سلسله مراتبی در شبیه ساز OPNET	الف-۶
۱۵۱	ویرایشگر شبکه ( Network editor or Project editor )	الف-۶-۱
۱۵۴	پنجره Object palette	الف-۶-۱-۱
۱۵۵	رسم ساختار شبکه در محیط ویرایشگر شبکه	الف-۶-۱-۲
۱۵۵	مشخص کردن پارامترهای مورد نظر برای اجرای شبیه سازی	الف-۶-۱-۳
۱۵۶	ویرایشگر Node	الف-۶-۲
۱۵۸	انواع ماژول ها در ویرایشگر Node	الف-۶-۲-۱
۱۶۰	منوهای مختلف در ویرایشگر Node	الف-۶-۲-۲
۱۶۱	ویرایشگر Process	الف-۶-۳
۱۶۲	حالات موجود در دیاگرام STD	الف-۶-۳-۱
۱۶۲	بررسی منوهای موجود در ویرایشگر Process	الف-۶-۳-۲
۱۶۳	توابع تعریف شده در Porto-C	الف-۶-۳-۳
۱۶۴	ویرایشگر انتشار آنتن ( Antenna Pattern Editor )	الف-۷
۱۶۵	ویرایشگر فرمت پکت (Packet Format Editor)	الف-۸

۱۶۶	عملیات ویرایشگر فرمت پکت	الف-۸-۱
۱۶۷	مشاهده و تحلیل نتایج شبیه سازی	الف-۹
۱۶۸		منابع

### فهرست شکل ها

۲۲	شکل ۱-۲ شبکه های Ad hoc
۲۲	شکل ۲-۲ (الف) نحوه ارتباط گره ها در یک حوزه ارتباطی (ب) ارتباط گره B با خارج از حوزه ارتباطی
۲۸	شکل ۳-۲: چگونگی ارتباط بین دو ایستگاه
۲۸	شکل ۴-۲: نمونه ای از یک ارتباط multi hop
۴۴	شکل ۱-۳ مسیریابی کوتاهترین مسیر با الگوریتم دایجکسترا
۴۵	شکل ۳-۳ (الف) یک زیر شبکه (ب) جداول دریافتی از همسایگان J و جدول مسیریابی جدید در J
۴۷	شکل ۳-۳ مشکل ( شمارش تا بی نهایت ) - عدم همگرایی سریع
۵۰	شکل ۴-۳ (الف) یک زیر شبکه (ب) بسته های حالت لینک (LS) برای این زیر شبکه
۵۲	شکل ۵-۳ یک شبکه WAN که شبکه های LAN، MAN و سلولهای بی سیم بدان متصل شده اند
۵۴	شکل ۶-۳ مسیریابی بسته ها بسوی ماشین های متحرک
۶۱	شکل ۱-۴ طبقه بندی پروتکل های مسیریابی در شبکه های اقتضائی
۶۴	شکل ۲-۴ جدول مسیریابی یک گره در روش DSDV در دو زمان متوالی
۶۷	شکل ۳-۴ یک نمونه سلسله مراتب در روش HSR
۷۰	شکل ۴-۴ نمونه ای از مکانیزم ایجاد مسیر در TORA
۷۱	شکل ۵-۴ نگهداری مسیر در TORA
۷۵	شکل ۶-۴ طبقه بندی پروتکل های مسیریابی در شبکه های اقتضائی
۷۶	شکل ۷-۴ طبقه بندی نسبتاً جامع پروتکل های مسیریابی در شبکه های اقتضائی
۷۹	شکل ۸-۴ پیغامهای درخواست مسیر و پاسخ مسیر برای مسیریابی
۷۹	شکل ۹-۴ مکانیزم کشف مسری در پروتکل مسیریابی از مبدا پویا: گره A سعی در بدست آوردن مسری به E دارد
۷۹	شکل ۱۰-۴ کشف مسیر در پروتکل مسیریابی از مبدا پویا از گره A تا D (DP:Data Packet)
۸۱	شکل ۱۱-۴ نمونه ای از نگهداری مسری در DSR که گره C قادر به ارسال بسته A به E نیست
۸۱	شکل ۱۲-۴ نگهداری مسیر در پروتکل مسیریابی از مبدا پویا (DP:Data Packet)
۸۲	شکل ۱۳-۴ نمونه ای از مکانیزم کشف مسیر در پروتکل مسیریابی از مبدا پویا
۸۳	شکل ۱۴-۴ فاز نگهداری مسری در پروتکل مسیریابی از مبدا پویا

- شکل ۴-۱۵ مسیریابی از گره S تا D در پروتکل مسیریابی از مبداء پویا (ارسال بسته های درخواست مسیر و دریافت بسته پاسخ مسیر و ارسال داده) ۸۴
- شکل ۴-۱۶ مثال از کاربرد حافظه نهان نودها در پروتکل مسیریابی از مبداء پویا ۸۵
- شکل ۴-۱۷ نمایی از پروتکل مسیریابی AODV ۸۸
- شکل ۴-۱۸ قالب بسته درخواست مسیر ۸۹
- شکل ۴-۱۹ قالب بسته پاسخ مسیر ۹۰
- شکل ۴-۲۰ (الف) گراف پس از حذف G از شبکه (ب) جدول مسیریابی D قبل از آن که G از کار بیفتد ۹۱
- شکل ۴-۲۱ یک مثال از پروتکل AODV - مسیریابی و ارسال داده از گره S تا گره D ۹۳
- شکل ۴-۲۲ پیدا کردن گره های ارسال چند نقطه ای در پروتکل مسیریابی حالت پیوند بهینه ۹۶
- شکل ۴-۲۳ کشف همسایه - تا دو گام همسایه ها را شناسایی می کند ۹۷
- شکل ۴-۲۴ پیدا کردن نود ارسال چند نقطه ای - شناسایی همسایه ها تا دو گام ۹۷
- شکل ۴-۲۵ انتخاب نود ارسال چند نقطه ای در پروتکل مسیریابی حالت پیوند بهینه ۹۸
- شکل ۴-۲۶ ارسال مجدد پخش کردن پکت ها تنها از طریق نقاط ارسال چند نقطه ای در پروتکل مسیریابی حالت پیوند بهینه ۹۹
- شکل ۴-۲۷ ارسال پیام به همسایه ها برای آگاه شدن از انتخاب آنها به عنوان نقاط ارسال چند نقطه ای در پروتکل مسیریابی حالت پیوند بهینه ۹۹
- شکل ۵-۱ نمایش دهنده تاخیر انتها به انتها ۱۰۵
- شکل ۵-۲ اجرای نرم افزار ، ایجاد محیط شبکه و قسمت تجهیزات شبکه ۱۰۷
- شکل ۵-۳ قسمت تجهیزات شبکه و وارد کردن ۲۰ نود متحرک ۱۰۸
- شکل ۵-۴ آوردن یک سرور ثابت و آدرس دهی IPv4 ۱۰۸
- شکل ۵-۵ انتخاب نودها و ایجاد پروتکل AODV ۱۰۸
- شکل ۵-۶ انتخاب Application \_ config ۱۰۹
- شکل ۵-۷ انتخاب پروتکل FTP ۱۰۹
- شکل ۵-۸ انتخاب Profile\_Config ۱۰۹
- شکل ۵-۹ تنظیمات Profile\_Config و آوردن قسمت تعریف تجهیزات ۱۱۰
- شکل ۵-۱۰ تعریف تجهیزات ( نودهای متحرک و سرور ثابت) در قسمت مربوطه ۱۱۰
- شکل ۵-۱۱ انتخاب Mobility\_Config ۱۱۰
- شکل ۵-۱۲ تنظیمات Mobility\_Config و اعمال تنظیمات آن در شبکه ۱۱۱
- شکل ۵-۱۳ مشاهده جهت حرکت نودها و انتخاب قسمت انتخاب پروتکل ها برای مشاهده نتایج بعد از شبیه سازی ۱۱۱
- شکل ۵-۱۴ انتخاب پروتکل ها برای دیدن نتایج بعد از شبیه سازی و انتخاب سناریوی بعدی ۱۱۱

- ۱۱۲ شکل ۵-۱۵ انتخاب نام سناریوی بعدی و انتخاب قسمت مشخصات نودها
- ۱۱۲ شکل ۵-۱۶ انتخاب پروتکل DSR و انتخاب قسمت انتخاب پروتکل ها برای مشاهده نتایج بعد از شبیه سازی
- ۱۱۲ شکل ۵-۱۷ انتخاب پروتکل ها برای مشاهده نتایج بعد از شبیه سازی و انتخاب سناریوی بعدی
- ۱۱۳ شکل ۵-۱۸ انتخاب نام سناریوی بعدی و انتخاب قسمت مشخصات نودها
- ۱۱۳ شکل ۵-۱۹ انتخاب پروتکل OLSR و انتخاب قسمت انتخاب پروتکل ها برای مشاهده نتایج بعد از شبیه سازی
- ۱۱۳ شکل ۵-۲۰ اجرای شبیه سازی ( ۳ سناریو )
- ۱۱۴ شکل ۵-۲۱ اجرای شبیه سازی ( ۱۲ سناریو )
- ۱۱۴ شکل ۵-۲۲ مشاهده نتایج شبیه سازی
- ۱۱۵ شکل ۵-۲۳ نمایی از محیط های شبکه
- ۱۱۶ شکل ۵-۲۴ نتایج زمان تاخیر AODV در ۴ محیط
- ۱۱۷ شکل ۵-۲۵ نتایج میزان سربار شبکه در AODV در ۴ محیط
- ۱۱۷ شکل ۵-۲۶ نتایج بار شبکه در AODV در ۴ محیط
- ۱۱۸ شکل ۵-۲۷ نتایج توان شبکه در AODV در ۴ محیط
- ۱۱۹ شکل ۵-۲۸ نتایج زمان تاخیر DSR در ۴ محیط
- ۱۱۹ شکل ۵-۲۹ نتایج میزان سربار شبکه در DSR در ۴ محیط
- ۱۲۰ شکل ۵-۳۰ نتایج بار شبکه در DSR در ۴ محیط
- ۱۲۱ شکل ۵-۳۱ نتایج توان شبکه در DSR در ۴ محیط
- ۱۲۱ شکل ۵-۳۲ نتایج زمان تاخیر OLSR در ۴ محیط
- ۱۲۲ شکل ۵-۳۳ نتایج میزان سربار شبکه در OLSR در ۴ محیط
- ۱۲۳ شکل ۵-۳۴ نتایج بار شبکه در OLSR در ۴ محیط
- ۱۲۴ شکل ۵-۳۵ نتایج توان شبکه در OLSR در ۴ محیط
- ۱۲۵ شکل ۵-۳۶ نتایج میزان تاخیر در محیط ۱ - AODV, DSR, OLSR
- ۱۲۵ شکل ۵-۳۷ نتایج میزان سربار شبکه در محیط ۱ - AODV, DSR, OLSR
- ۱۲۶ شکل ۵-۳۸ نتایج بار شبکه در محیط ۱ - AODV, DSR, OLSR
- ۱۲۶ شکل ۵-۳۹ نتایج توان شبکه در محیط ۱ - AODV, DSR, OLSR
- ۱۲۷ شکل ۵-۴۰ نتایج میزان تاخیر در محیط ۲ - AODV, DSR, OLSR
- ۱۲۷ شکل ۵-۴۱ نتایج میزان سربار شبکه در محیط ۲ - AODV, DSR, OLSR
- ۱۲۸ شکل ۵-۴۲ نتایج بار شبکه در محیط ۲ - AODV, DSR, OLSR
- ۱۲۸ شکل ۵-۴۳ نتایج توان شبکه در محیط ۲ - AODV, DSR, OLSR
- ۱۲۹ شکل ۵-۴۴ نتایج میزان تاخیر در محیط ۳ - AODV, DSR, OLSR

- شکل ۴۵-۵ نتایج میزان سرشار شبکه در محیط ۳ - AODV, DSR, OLSR ۱۲۹
- شکل ۴۶-۵ نتایج بار شبکه در محیط ۳ - AODV, DSR, OLSR ۱۳۰
- شکل ۴۷-۵ نتایج توان شبکه در محیط ۳ - AODV, DSR, OLSR ۱۳۰
- شکل ۴۸-۵ نتایج میزان تاخیر در محیط ۴ - AODV, DSR, OLSR ۱۳۱
- شکل ۴۹-۵ نتایج میزان سرشار شبکه در محیط ۴ - AODV, DSR, OLSR ۱۳۱
- شکل ۵۰-۵ نتایج بار شبکه در محیط ۴ - AODV, DSR, OLSR ۱۳۲
- شکل ۵۱-۵ نتایج توان شبکه در محیط ۴ - AODV, DSR, OLSR ۱۳۲
- شکل ۵۲-۵ نتایج میزان تاخیر در ۱۲ سناریو ( همه تاخیر زمان ها) - AODV, DSR, OLSR ۱۳۳
- شکل ۵۳-۵ نتایج میزان سرشار شبکه در ۱۲ سناریو ( همه میزان سرشارها) - AODV, DSR, OLSR ۱۳۴
- شکل ۵۴-۵ نتایج بار شبکه در ۱۲ سناریو ( همه نتایج در یک نمودار) - AODV, DSR, OLSR ۱۳۴
- شکل ۵۵-۵ نتایج توان شبکه در ۱۲ سناریو ( همه نتایج در یک نمودار) - AODV, DSR, OLSR ۱۳۵
- شکل ۵۶-۵ نتایج میزان تاخیر شبکه در محیط ۶۵ - AODV, DSR, OLSR ۱۳۶
- شکل ۵۷-۵ نتایج میزان سرشار شبکه در محیط ۶۵ - AODV, DSR, OLSR ۱۳۶
- شکل ۵۸-۵ نتایج بار شبکه در محیط ۶۵ - AODV, DSR, OLSR ۱۳۷
- شکل ۵۹-۵ نتایج توان شبکه در محیط ۶۵ - AODV, DSR, OLSR ۱۳۸
- شکل الف-۱ چهار مرحله شبیه سازی توسط نرم افزار opnet ۱۴۶
- شکل الف-۲ میزان استفاده از شبیه سازهای مختلف بمنظور شبیه سازی شبکه های MANET ۱۴۷
- شکل الف-۳ نرم افزار رایگان OPNET 9.1 - IT Guru Academic Edition ۱۴۹
- شکل الف-۴ پنجره شروع به کار نرم افزار OPNET ۱۵۰
- شکل الف-۵ ساختار سلسله مراتبی در OPNET ۱۵۱
- شکل الف-۶ انتخاب و وارد شدن به محیط ویرایشگر شبکه ۱۵۲
- شکل الف-۷ انتخاب ساختار شبکه بر مبنای یک ساختار قبلی ۱۵۲
- شکل الف-۸ انتخاب مشخصات جغرافیایی شبکه ۱۵۳
- شکل الف-۹ تکنولوژی ادوات مورد استفاده ۱۵۳
- شکل الف-۱۰ نمایش تمامی اطلاعات انتخاب شده در مراحل قبل برای تایید نهایی ۱۵۳
- شکل الف-۱۱ محیط ویرایشگر شبکه ۱۵۴
- شکل الف-۱۲ پنجره object Palette ۱۵۵
- شکل الف-۱۳ تعیین پارامترهای مورد نیاز برای اجرای شبیه سازی پارامترهای خصوصی و عمومی ۱۵۶
- شکل الف-۱۴ محیط ویرایشگر Nod ۱۵۷
- شکل الف-۱۵ انواع اتصال ماژول ها ۱۵۸



۱۵۸	شکل الف-۱۶ مازول پردازشگر
۱۵۸	شکل الف-۱۷ مازول صف
۱۵۹	شکل الف-۱۸ انواع مازول های فرستنده
۱۵۹	شکل الف-۱۹ انواع مازول های گیرنده
۱۵۹	شکل الف-۲۰ مازول آنتن و نحوه تعاملات آنتن ها
۱۶۱	شکل الف-۲۱ دیاگرام STD
۱۶۲	شکل الف-۲۲ حالت های موجود در دیاگرام STD
۱۶۳	شکل الف-۲۳ نحوه نامگذاری توابع KP
۱۶۵	شکل الف-۲۴ نمایش پارامترهای ویرایشگر انتشار آنتن
۱۶۵	شکل الف-۲۵ محیط ویرایشگر آنتن
۱۶۶	شکل الف-۲۶ محیط ویرایشگر Packet Format
۱۶۷	شکل الف-۲۷ پنجره مشاهده نتایج

### فهرست جداول

۱۳۸	جدول ۵-۱ نتایج آماری کل شبیه سازی در ۶ محیط
۱۶۰	جدول الف-۱ گزینه های موجود در منوی interfaces
۱۶۱	جدول الف-۲ گزینه های موجود در منوی windows

## فصل اول

### پیشگفتار

## ۱-۱ پیشگفتار

شبکه های اقتضائی متحرک نمونه ی نوینی از شبکه های مخابراتی بی سیم هستند که به خاطر مشخصات منحصر به فردشان امروزه بسیار مورد توجه قرار گرفته ان . در این شبکه ها هیچ پایگاه مبناء تقویت کننده و مرکز سوئیچینگ ثابتی وجود ندارد ، بلکه این خود گره ها هستند که عملیات تقویت داده ، سوئیچینگ و مسیریابی را انجام می دهند. با توجه به تغییرات مداوم در توپولوژی شبکه به واسطه ی تحرک گره ها ، پروتکل های مسیریابی باید با اتخاذ نوعی استراتژی سازگار این تغییرات را پشتیبانی نمایند ، به نحوی که داده ی ارسالی به سلامت از مبدا به مقصد برسد . از اوایل دهه ۸۰ میلادی تاکنون پروتکل های مسیریابی فراوانی برای شبکه های اقتضائی پیشنهاد شده است . این پروتکل ها رنج وسیعی از مبانی و روش های طراحی را شامل می شوند . از یک تعریف ساده برای پروتکل های اینترنتی گرفته تا روش های سلسله مراتبی چندسطحی پیچیده . بسیاری از این پروتکل ها بر اساس فرض های ابتدایی ساده ای طراحی می شوند ، مثلاً در بسیاری از این پروتکل ها تمام گره ها منابع و توانایی های یکسانی دارند ، به عنوان نمونه گره ها رنج ارسال یکسان دارند و پیوندها دوطرفه فرض می شوند ، البته پروتکل هایی هم هستند که عملاً با لینک های یک طرفه سروکار دارند. نهایتاً اگرچه هدف بسیاری از پروتکل ها قابل استفاده بودن برای شبکه های بزرگ است اما معمولاً و به طور میانگین برای ۱۰ تا ۱۰۰ گره طراحی می شوند. کمبود توان باتری ، پهنای باند محدود ، میزان خطای زیاد و تغییرات مداوم در توپولوژی شبکه از مشکلات شبکه های اقتضائی می باشد. به دلیل همین محدودیت ها پروتکل های مسیریابی برای این گونه شبکه ها به گونه ای طراحی می شوند که حداقل یکی از عوامل زیان بار شبکه را کمینه سازند. به عنوان مثال برخی پروتکل ها صرفاً بر مبنای توان باتری گره ها بنا می شوند، بسیاری دیگر کمینه سازی سربارهای پردازشی را مورد توجه قرار می دهند و در بسیاری دیگر اجتناب از حلقه (که خود عامل بسیاری از محدودیت ها در شبکه من جمله کاهش پهنای باند و ... است) هدف طراحی است. اما دسته وسیعی از پروتکل ها نیز وجود دارند که به دنبال کمینه سازی سربارهای کنترلی هستند. در این پایان نامه در سه فصل اول به بررسی شبکه های اقتضائی و پروتکل های مسیریابی پرداخته شده است. سپس در فصل بعدی با استفاده از نرم افزار شبیه سازی ، شش محیط شبکه اقتضائی با نودهای متحرک پیاده سازی شده و پروتکل های مسیریابی AODV , DSR , OLSR در این شبکه ، با استفاده از نتایج ، مورد تحلیل و بررسی قرار گرفته است. همچنین در پیوست برای علاقه مندان به آشنایی با محیط این شبیه ساز ، آموزش مختصری قرار دارد .

## فصل دوم

### شبکه های اقتضائی متحرک

## ۲-۱ مقدمه

شبکه های اقتضائی به شبکه های آنی و یا موقت گفته می شود که برای یک منظور خاص به وجود می آیند. در واقع شبکه های بی سیم هستند که گره های آن متحرک می باشند. تفاوت عمده شبکه های اقتضائی با شبکه های معمول بی سیم 802.11 در این است که در شبکه های اقتضائی مجموعه ای از گره های متحرک بی سیم بدون هیچ زیرساختار مرکزی، نقطه دسترسی و یا ایستگاه پایه برای ارسال اطلاعات بی سیم در بازه ای مشخص به یکدیگر وصل می شوند. ارسال بسته های اطلاعاتی در شبکه های بی سیم اقتضائی توسط گره های مسیری که قبلاً توسط یکی از الگوریتم های مسیریابی مشخص شده است، صورت می گیرد. نکته قابل توجه این است که هر گره تنها با گره هایی در ارتباط است که در شعاع رادیویی اش هستند، که اصطلاحاً گره های همسایه نامیده می شوند. پروتکل های مسیریابی بر اساس پارامترهای کانال مانند تضعیف، انتشار چند مسیره، تداخل و همچنین بسته به کاربرد شبکه به صورت بهینه طراحی شده اند. در هنگام طراحی این پروتکلها به امر تضمین امنیت در شبکه های اقتضائی توجه نشد. در سالهای اخیر با توجه به کاربردهای حساس این شبکه از جمله در عملیتهای نظامی، فوریت های پزشکی و یا مجامع و کنفرانسها، که نیاز به تامین امنیت در این شبکه ها بارزتر شده است، محققان برای تامین امنیت در حیطه عملکرد پیشنهادات گوناگونی را مطرح می کنند. شبکه های بی سیم اقتضائی فاقد هسته مرکزی برای کنترل ارسال و دریافت داده می باشد و حمل بسته های اطلاعاتی به شخصه توسط خود گره های یک مسیر مشخص و اختصاصی صورت می گیرد. توپولوژی شبکه های اقتضائی متغیر است زیرا گره های شبکه می توانند تحرک داشته باشند و در هر لحظه از زمان جای خود را تغییر بدهند.

## ۲-۲ شبکه های بی سیم

شبکه محلی بی سیم یا WLAN به نوعی از شبکه محلی اطلاق می شود که در آن برای انتقال اطلاعات از یک نقطه به نقطه دیگر از امواج رادیویی استفاده شود. مزیت مهم یک شبکه بی سیم این است که نیاز به سیم کشی ندارد و در نتیجه کاربران می توانند در محدوده شبکه جابجا شوند. هر شبکه بیسیم برای خود یک برد موثر دارد که به عواملی مانند تجهیزات و استانداردهای رعایت شده بستگی دارد و اگر یکی از کاربران شبکه از آن برد خارج شود قادر به ارسال اطلاعات نیست.

## ۲-۳ امنیت شبکه



شبکه های بی سیم به علت ماهیت خاص خود بسیار در معرض دسترسی های غیرمجاز قرار دارند. این شبکه ها به شدت در مقابل حملات آسیب پذیرند و امروزه مقاومت کردن در برابر حملات از چالش های توسعه این شبکه هاست. دلایل اصلی این مشکلات عبارتند از :

- (۱) کانال رادیویی اشتراکی انتقال داده
- (۲) محیط عملیاتی ناامن
- (۳) قدرت مرکزی ناکافی
- (۴) منابع محدود
- (۵) آسیب پذیر بودن از لحاظ فیزیکی
- (۶) کافی نبودن ارتباط نودهای میانی.

ساختار این شبکه ها مبتنی بر استفاده از سیگنال های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه چندان قدرتمند این شبکه ها، خود را به عنوان عضوی از این شبکه ها جازده و در صورت تحقق این امر، امکان دستیابی به اطلاعات حیاتی، حمله به سرویس دهنده گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره های شبکه با یکدیگر، تولید داده های غیر واقعی و گمراه کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت های مخرب وجود دارد. در مجموع، در تمامی دسته های شبکه های بی سیم، از دید امنیتی حقایق مشترک صادق است :

- (۱) نفوذگران، با گذر از تدابیر امنیتی موجود، می توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم های رایانه ای دست یابند.
- (۲) حمله های DOS به تجهیزات و سیستم های بی سیم بسیار متداول است.
- (۳) کامپیوترهای قابل حمل و جیبی، که امکان استفاده از شبکه بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می توان اولین قدم برای نفوذ به شبکه را برداشت.
- (۴) یک نفوذگر می تواند از نقاط مشترک میان یک شبکه بی سیم در یک سازمان و شبکه سیمی آن (که در اغلب موارد شبکه اصلی و حساس تری محسوب می گردد) استفاده کرده و با نفوذ به شبکه بی سیم عملاً راهی برای دست یابی به منابع شبکه سیمی نیز بیابد.

## ۴-۲ توپولوژی های شبکه بی سیم

در استاندارد تعیین شبکه برای شبکه های محلی بی سیم از دو روش برای ساختن شبکه استفاده می شود .

(۱) مدل Ad Hoc یا (Independent basic service set)

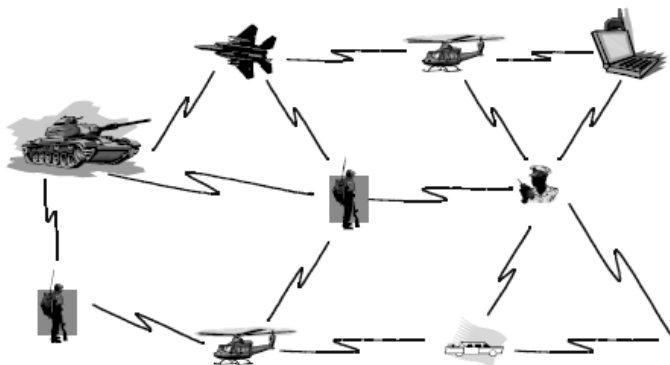
(۲) مدل Infra Structure یا (Basic Service Set)

## ۲-۴-۱ مدل Infra Structure یا (Basic Service Set)

توپولوژی ثابت شبکه ، در شبکه زیرساخت مستقر شده است. شبکه های دارای زیرساخت دارای ایستگاه های پایه یا نقاط دسترسی برای اتصال گره های بی سیم می باشند. تمام ایستگاه های پایه و یا نقاط دسترسی از طریق لینک های سیمی (فیبر نوری، پیچ خورده و یا کابل هم محور) و یا لینک های بی سیم به شبکه اصلی متصل می شوند. ایستگاه پایه یا نقطه دسترسی، یکی از واحدهای مهم شبکه های زیرساخت است. همه اتصالات مجبور به عبور از نقطه دسترسی می باشند . گره های بی سیم می توانند به هر کسی با استفاده از نقاط دسترسی در محدوده رادیویی خود ارتباط برقرار کنند.

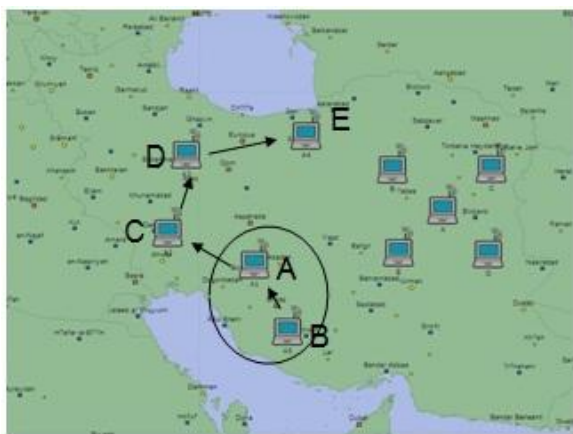
## ۲-۴-۲ مدل ad-hoc

این اصطلاح که از زبان لاتین گرفته شده است به معنای برای کاربرد اختصاصی - اقتضائی است. این عبارت عموماً در مورد راه حلی استفاده می شود که برای حل یک مشکل خاص یا انجام وظیفه ای ویژه طراحی شده باشد و قابل تعمیم به صورت یک راه حل عمومی نباشد و امکان تطبیق دادن آن با مسایل دیگر وجود نداشته باشد. شبکه بندی اقتضائی یک ایده جدید نیست. به عنوان یک تکنولوژی برای شبکه های بی سیم پویا برای مقاصد نظامی از سال ۱۹۷۰ گسترش پیدا کرده است. دستگاهها در این شبکه می توانند در هر زمانی و در هر جایی بدون استفاده از یک ساختار مرکزی با هم ارتباط برقرار کنند ، به عبارتی شبکه ای است بدون هیچ گونه مدیریت مرکزی و متشکل از نودهای متحرک که از یک ارتباط بیسیم برای ارسال داده ها استفاده می نماید . یک شبکه اقتضائی ، اتصالی است که تنها به مدت یک جلسه برقرار می شود و نیاز به ایستگاه پایه ندارد. در عوض، هر دستگاه متصل به شبکه، دیگر دستگاه های واقع در یک محدوده خاص را پیدا می کند و این دستگاه ها یک شبکه بین خود ایجاد می کنند. از سوی دیگر دستگاه ها با ارسال پیام، گره های هدف را در خارج از محدوده تعریف شده جستجو می کنند. امکان برقراری ارتباط بین چندین گره مختلف وجود دارد. به این ترتیب، شبکه های اقتضائی گوناگون به یکدیگر متصل می شوند. سپس پروتکل های مسیریابی، اتصالات پایداری را بین این گره ها ایجاد می کنند، حتی اگر گره ها متحرک باشند.

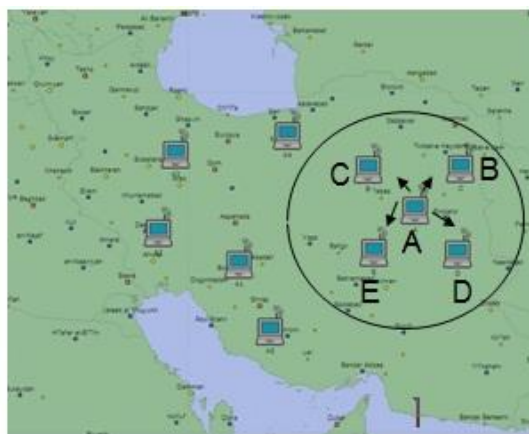


شکل ۱-۲ شبکه های Ad hoc

در یک شبکه اقتضائی خبری از زیرساخت های ثابت همچون پایگاه های مبنا و مراکز سوئیچینگ و تقویت کننده ثابت نیست. گره های متحرکی که در حوزه ارتباطی یکدیگر قرار دارند مستقیماً از طریق لینک بی سیم با هم مرتبط می شوند در حالی که گره هایی که از هم دورند پیام شان از طریق دیگر گره ها تقویت شده تا به گره مقصد برسند.



(الف)



(ب)

شکل ۲-۲ (الف) نحوه ارتباط گره ها در یک حوزه ارتباطی (ب) ارتباط گره B با خارج از حوزه ارتباطی در شکل ۲-۲ الف بطور مستقیم با همه ارتباط برقرار می کند ولی در شکل ۲-۲ ب گره B برای ارتباط با گره E باید از گره های A و C و D کمک بگیرد و از طریق آن ها با گره E ارتباط برقرار نماید.

Ad-hoc از آغاز تا کنون:

1968 ALOHA

1973 ( packet radio network) PRnet توسط DARPA

1980 SURAN

1990 802.11 کارتهای رادیویی

شبکه های Ad hoc تاسیسات نظامی

## ۲-۵ شبکه های اقتضائی بی سیم

یک شبکه اقتضائی بیسیم یک شبکه بیسیم غیرمتمرکز است. این شبکه شامل مجموعه ای از گره های توزیع شده است که بدون هیچ زیرساخت یا مدیریت مرکزی، یک شبکه موقت را تشکیل می دهند. در این شبکه ها، هیچ زیرساختی مثل مسیریاب یا نقطه دسترسی وجود ندارد، بلکه گره ها به طور مستقیم با هم ارتباط برقرار می کنند و هر گره از طریق ارسال داده ها برای سایر گره ها در مسیریابی شرکت می کند. در شبکه های اقتضائی، گره ها می توانند هم به عنوان مسیریاب و هم به عنوان میزبان عمل کنند. شبکه موردی به دستگاه ها این امکان را می دهد که در هر زمان و در هر مکان بدون نیاز به یک زیرساخت مرکزی با یکدیگر ارتباط برقرار کنند. شبکه های اقتضائی یا موردی به دلایل نظامی به وجود آمدند اما امروزه در صنعت و بسیاری از مقاصد غیرنظامی استفاده می شوند. به دلیل تحرک گره ها، توپولوژی شبکه پویا و متغیر می باشد. بنابراین، با توجه به این که گره ها می توانند به طور پیوسته موقعیت خود را تغییر دهند، به یک پروتکل مسیریابی که توانایی سازگاری با این تغییرات را داشته باشد، نیاز دارد. در یک شبکه موردی، گره ها از طریق لینک های بی سیم به هم متصل شده اند. از آنجایی که لینک ها می توانند در هر زمان متصل یا منفصل شوند، یک شبکه باید قادر باشد خود را با ساختار جدید تطبیق دهد. یک مسیر دنباله ای از لینک ها است که دو گره را به هم متصل می کند. برخلاف شبکه های زیرساخت، در شبکه های موردی، مسیریابی به صورت چندگامی است. در شبکه های زیرساخت، کاربر تنها در یک گام با ایستگاه مرکزی ارتباط برقرار میکند و ایستگاه مرکزی، پیام مربوطه را به کاربر دیگر می رساند. اما در شبکه های موردی، یک کاربر از طریق چند گام با کاربر دیگر ارتباط برقرار میکند. گام ها گره های میانی هستند که وظیفه شان تقویت و ارسال پیام ها از مبدا به مقصد است. گره هایی که در حوزه ارتباطی یکدیگر قرار دارند، مستقیماً از طریق لینک های بی سیم با هم ارتباط برقرار می کنند و گره هایی که از هم دورند، پیامشان از طریق گره های میانی تقویت و ارسال می شود تا به گره مقصد برسد. این شبکه ها قادر به خودپیکربندی هستند. به طوری که اگر یکی از گره های میانی با مشکل مواجه شود، شبکه به طور خودکار مجدداً خود را پیکربندی کرده و یک مسیر جایگزین را از مبدا به مقصد تعیین می کند. به منظور پیکربندی شبکه، ابتدا هر گره، گره هایی که برای ارتباط در دسترس هستند را شناسایی می کند. سپس هر گره اطلاعات بدست آمده را به همراه مقصد مورد نظر، برای سایر گره ها ارسال می کند. الگوریتم پیکربندی شبکه با استفاده از لیستی از اتصالات موجود، یک مسیریابی منحصر بفرد را برای ارتباط هر کاربر با مقصدش بر می گزیند. با گذشت زمان، شبکه تغییر می کند. کاربران ممکن است بیایند و بروند، گره ها ممکن است جابجا شوند یا تغییر در محیط الکترومغناطیس ممکن

است انتشار بین گره ها را دچار تغییر کند. هنگامی که این تغییرات رخ می دهند، شبکه پیکربندی خود را به روز رسانی می کند و مسیرهای جدیدی را از کاربران به مقاصدشان شناسایی می کند. این پیکربندی مجدد، در طی تغییرات شبکه بارها و بارها تکرار می شود. به این ترتیب شبکه های موردی قادر به خودترمیمی می باشند که این قابلیت از طریق خودپیکربندی مداوم شبکه فراهم می شود.

## ۲-۵-۱ خصوصیات شبکه های اقتضائی

شبکه های بی سیم دارای نیازمندیها و مشکلات امنیتی ویژه ای هستند. این مشکلات ناشی از ماهیت و خواص شبکه های بی سیم است که در بررسی هر راه حل امنیتی باید به آنها توجه نمود:

(۱) فقدان زیرساخت : در شبکه های بی سیم ساختارهای متمرکز و مجتمع مثل سرورس دهنده ها، مسیریابها

و... لزوماً موجود نیستند (مثلاً در شبکه های اقتضائی)، به همین خاطر راه حل های امنیتی آنها هم معمولاً

غیر متمرکز، توزیع شده و مبتنی بر همکاری همه نودهای شبکه است.

(۲) استفاده از لینک بی سیم: در شبکه بی سیم، خطوط دفاعی معمول در شبکه های سیمی (مثلاً فایروال به

عنوان خط مقدم دفاع) وجود ندارد. نفوذگر از تمام جهتها و بدون نیاز به دسترسی فیزیکی به لینک،

می تواند هر نودی را هدف قرار دهد.

(۳) چند پرشی بودن: در اغلب پروتکل های مسیریابی بی سیم، خود نودها نقش مسیریاب را ایفا می کنند (به

خصوص در شبکه های اقتضائی)، و بسته ها دارای چند گام مختلف هستند. طبیعتاً به هر نودی نمی توان

اعتماد داشت آن هم برای وظیفه ای همچون مسیریابی!

(۴) خودمختاری نودها در تغییر مکان: نودهای سیار در شبکه بی سیم به دلیل تغییر محل به خصوص در

شبکه های بزرگ به سختی قابل ردیابی هستند.

از دیگر ویژگیهای طبیعی شبکه بی سیم که منبع مشکلات امنیتی آن است می توان به فقدان توپولوژی ثابت و

محدودیت های منابعی مثل توان، پردازنده و حافظه اشاره کرد. مهمترین ویژگی این شبکه ها وجود یک

توپولوژی پویا و متغیر میباشد که نتیجه تحرک نودها می باشد. نودها در این شبکه ها به طور پیوسته موقعیت

خود را تغییر میدهند که این خود نیاز به یک پروتکل مسیریابی که توانایی سازگاری با این تغییرات را داشته،

نمایان میکند.

## ۲-۵-۲ انواع شبکه های اقتضائی بی سیم



۱) شبکه های موردی (اقتضائی) سیار<sup>۱</sup> (MANET)

۲) شبکه های حسگر بی سیم<sup>۲</sup> (WSN)

۳) شبکه های توری بی سیم<sup>۳</sup> (WMN)

## ۲-۵-۱-۲ شبکه های موردی (اقتضائی) سیار

یک شبکه اقتضائی سیار (MANET)، یک شبکه بدون زیرساخت و دارای قابلیت خودپیگر بندی است که از دستگاه های متحرکی که از طریق لینک های بی سیم به هم متصل شده اند، تشکیل شده است. هر دستگاه موجود در یک شبکه های اقتضائی متحرک آزاد است که به طور مستقل در هر جهتی حرکت کند و در نتیجه لینک های آن به سایر دستگاه ها مکررا تغییر می کنند. دستگاه ها شامل مسیریاب ها و میزبان های متحرک می باشند که یک گراف دلخواه را تشکیل می دهند. شبکه های اقتضائی متحرک ممکن است به صورت مستقل عمل کنند یا به شبکه دیگری مثل اینترنت متصل باشند. شبکه موردی وسایل نقلیه<sup>۴</sup>، نوعی شبکه های اقتضائی متحرک است که برای ارتباط میان وسایل نقلیه و همچنین ارتباط بین وسایل نقلیه و تجهیزات کنار جاده ای بکار می رود.

## ۲-۵-۲ شبکه های حسگر بی سیم

در مسیریابی در شبکه های اقتضائی نوع حسگر سخت افزار محدودیت هایی را بر شبکه اعمال می کند که باید در انتخاب روش مسیریابی مد نظر قرار بگیرند از جمله اینکه منبع تغذیه در گره ها محدود می باشد و در عمل، امکان تعویض یا شارژ مجدد آن مقدور نیست؛ لذا روش مسیریابی پیشنهادی در این شبکه ها بایستی از انرژی موجود به بهترین نحو ممکن استفاده کند یعنی باید مطلع از منابع گره باشد و اگر گره منابع کافی نداشته بسته را به آن برای ارسال به مقصد نفرستد. خودمختار بودن و قابلیت انطباق گره ها را ایجاد کند. متشکل از چندین سنسور هستند که در محدوده ی جغرافیایی معینی قرار گرفته اند. هر سنسور دارای قابلیت ارتباطی بیسیم و هوش کافی برای پردازش سیگنال ها و امکان شبکه سازی است. یک شبکه بیسیم که به صورت سه بعدی توزیع شده اند و برای حس کردن شرایط فیزیکی از سنسورهای مشترک استفاده می کنند.

نظارت محیطی، ردگیری، کنترل، نظارت زیستی، تشخیص آتش، نظارت ترافیک، نظارت ناحیه ای

انواع سنسور:

سنسورهای صوتی، لرزه نگار، مادون قرمز، دوربینهای ویدیویی

- 1 - Mobile Ad Hoc Network
- 2 - Wireless Sensor Network
- 3 - Wireless Mesh Network
- 4 - VANET

## ۲-۵-۳ شبکه های توری بی سیم

شبکه های توری بی سیم یا مش یک ساختار ارتباطی مشارکتی بی سیم بین تعداد بسیار زیادی از گیرنده فرستنده های بی سیم منفرد است که دارای قابلیت های نوع اترنت می باشد. این نوع از ساختار می تواند غیر متمرکز باشد (بدون سرور مرکزی) برای کاربردهای مقیاس محدود یا می تواند با کنترل مرکزی باشد برای کاربردهایی با قابلیت بالای افزایش مقیاس (با یک سرور مرکزی)

## ۲-۶ شبکه های اقتضائی متحرک

شبکه های اقتضائی متحرک مجموعه ای از نود های موبایل یا متحرک مجهز به گیرنده و فرستنده به منظور برقراری ارتباطات بی سیم می باشد. نود های موبایل به دلیل وجود محدودیت هایی در فرستنده و گیرنده های خود نمی توانند با تمام نود ها ارتباط مستقیم برقرار کنند. به همین دلیل لازم است در مواردی که امکان برقراری چنین ارتباط مستقیمی وجود ندارد داده ها از طریق بقیه ی نود ها که در این حالت نقش مسیر یاب را ایفا می کنند منتقل شوند. با این حال متحرک بودن نود ها باعث شده شبکه مدام در حال تغییر بوده و مسیر های مختلفی بین دو نودها به وجود آید. عوامل دیگری همچون اندازه ی بزرگ شبکه و نا همگونی انواع میزبان ها و تنوع نوع و ساختار آنها و محدودیت توان باتری ها طراحی پروتکل های مسیر یابی مناسب را به یک مشکل جدی بدل کرده است. برای این منظور بایستی از پروتکل های مناسب و امنی استفاده شود که در ادامه به آنها خواهیم پرداخت. همچنین نود ها هیچ دانش پیشینی نسبت به توپولوژی شبکه ای که در محدوده ی آنها برقرار است ندارند و بایستی از طریقی پی به آن ببرند. روش رایج این است که یک نود جدید بایستی حضور خود را اعلام کرده و به اطلاعات پخش شده از همسایگان خود گوش فرا دهد تا بدین ترتیب اطلاعاتی در مورد نودها های اطراف و نحوه ی دسترسی به آنها به دست آورد.

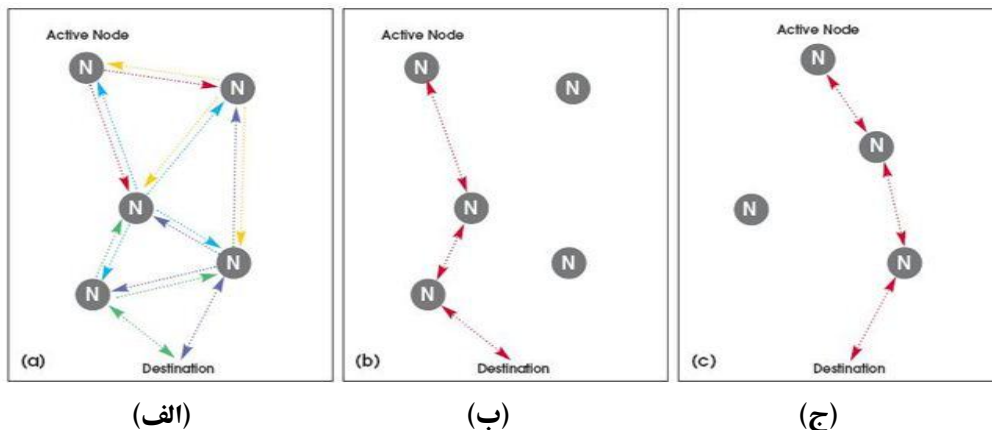
## ۲-۶-۱ ساختار شبکه های اقتضائی متحرک

شبکه های اقتضائی متحرک مجموعه ی مستقلی از کاربرین متحرک است که از طریق لینک های بی سیم با یکدیگر ارتباط برقرار می کنند. برای اتفاقات غیر قابل پیش بینی اتصالات، شبکه های متمرکز کارا نبوده و قابلیت اطمینان کافی را ندارند، لذا شبکه های اقتضائی متحرک راه حل مناسبی است همچنین در زمینه هایی که در آنها زیرساخت های ارتباطی وجود نداشته یا اینکه زیرساخت های موجود بسیار گران قیمت بوده و استفاده از آنها راحت نیست، کاربران سیار بی سیم می توانند از طریق شبکه های اقتضائی متحرک با یکدیگر ارتباط برقرار کنند. نود های واقع در شبکه های اقتضائی متحرک مجهز به گیرنده و فرستنده های بی سیم بوده و از آنتن هایی

استفاده می کنند که ممکن است از نوع فراگیر و یا نظیر به نظیر باشند. شبکه های اقتضائی متحرک مجموعه ای از نود های موبایل یا متحرک به منظور برقراری ارتباطات بی سیم است. شبکه موبایل سیار به عنوان شبکه های با عمر کوتاه شناخته می شود، شبکه تلفن همراه از گره هایی در غیاب هر گونه حمایت متمرکز تشکیل شده است. این یک فرم جدیدی از شبکه است و ارائه خدمات در مکان هایی که در آن امکان پذیر نمی باشد را ممکن می سازد. همچنین نودها هیچ دانش پیشینی نسبت به توپولوژی شبکه ای که در محدوده ی آنها برقرار است ندارند و بایستی از طریقی پی به آن ببرند... همچنین شبکه سیار موبایل یک شبکه بی سیم چندمرحله ای برنامه ریزی شده و پیکربندی شده است که مجموعه ای از گروه های سیار (MHs) را می سازد و بطور آزادانه حرکت کرده و با بسته های بازپخش برای همدیگر همکاری می کند. شبکه های اقتضائی متحرک از عملکردهای نتیجه بخش و دقیق بواسطه جادادن خطوط در حال کار بطرف MHs حمایت می کند، همچنین یک مسیر تک قالبی جلوبرنده چند مرحله ای را برای دو گره بیشتر از محدوده ارتباطی مستقیم بی سیم می سازد. مسیر پروتکل همچنین ارتباطات را وقتی که این ارتباط در این مسیر قطع می شود، حفظ می کند که دلیل آن تأثیر حرکت گره ای، دردسترس بودن باتری، پخش رادیویی، و مداخله وایرلس می باشد. نود های موبایل به دلیل وجود محدودیت هایی در فرستنده و گیرنده های خود نمی توانند با تمام نود ها ارتباط مستقیم برقرار کنند. به همین دلیل لازم است در مواردی که امکان برقراری چنین ارتباط مستقیمی وجود ندارد داده ها از طریق بقیه ی نود ها که در این حالت نقش مسیر یاب را ایفا می کنند منتقل شوند. با این حال متحرک بودن نود ها باعث شده شبکه مدام در حال تغییر بوده و مسیرهای مختلفی بین دو نود به وجود آید. آنچه که این شبکه ها را با سایر شبکه های مشابه متمایز می سازد، خصوصیات ذاتی آن می باشد که در ادامه به شرح آن می پردازم. به عنوان مثال در شبکه سلولی (تلفن همراه)، با وجود این که گره ها متحرک هستند و از طریق ارتباطات بی سیم با هم تبادل اطلاعات می کنند ولی زیر ساخت شبکه ای ثابتی باید وجود داشته باشد (BTS) تا شبکه سلولی بتواند به کار خود ادامه دهد در حالی که در شبکه های موردی هیچ زیرساخت ثابتی وجود ندارد. از اینرو برپایی شبکه های موردی سریعتر و هوشمندتر صورت می گیرد. نوع ترافیک در شبکه های سیار کاملاً متفاوت از شبکه بی سیم بر مبنای زیر ساختار است و شامل:

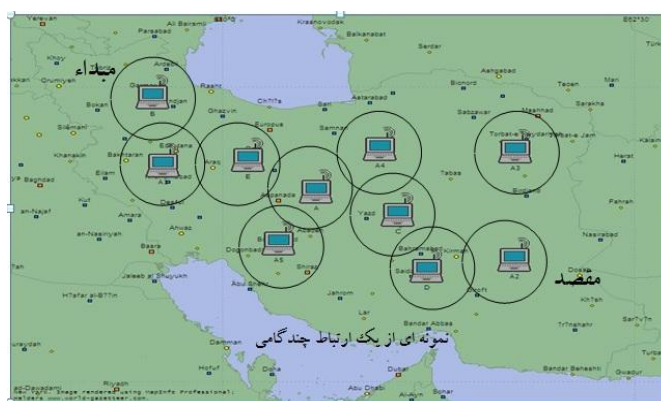
نظیر به نظیر: ارتباط بین دو گره ای که درون یک شعاع رادیویی هستند. ترافیک شبکه معمولاً ثابت است. ارتباط خارج از منطقه: ارتباط بین دو گره ای که آن سوی یک شعاع رادیویی هستند اما یک مسیر ثابت بین آن ها وجود دارد.

حرکت پویا: این هنگامی رخ می دهد که گره ها پویا هستند و حرکت می کنند و مسیرها باید دوباره ایجاد شوند. به شکل زیر توجه کنید:



شکل ۲-۳: چگونگی ارتباط بین دو ایستگاه

شکل ۲-۳ الف شناسایی گره ها توسط ایستگاه ها را نشان می دهد. در شکل ۲-۳ ب می بینیم که یکی از ایستگاه ها برای ارسال داده به سمت مقصد مورد نظرش از یک مسیر خاص و بهینه استفاده می کند. در شکل ۲-۳ ج وضعیتی نشان داده شده است که یکی از ایستگاههای میانی از شبکه خارج شده و در نتیجه بعد از انجام پیکربندی مجدد، مسیر دیگری بین مبدا و مقصد برای ارسال داده ها بوجود آمده است. برخلاف سیستمهای مخابراتی جاری شبکههای سیار شبکههای بی سیم چند گامی یا پرشی هستند، یعنی یک کاربر از طریق چند گام با کاربر دیگر ارتباط برقرار میکند (در حالیکه در سیستمهای کنونی کاربر تنها در یک گام با ایستگاه مرکزی ارتباط می یابد). نمونه ای از یک ارتباط چند گامی در شکل زیر آمده است:



شکل ۲-۴ نمونه ای از یک ارتباط multi hop

## ۲-۶-۲ خصوصیات شبکه های اقتضائی متحرک

شبکه های اقتضائی متحرک نیز مانند انواع شبکه های دیگر دارای ویژگی هایی است که از آن جمله می توان به موارد زیر اشاره کرد:

- (۱) ترمینال مستقل: در شبکه های اقتضائی متحرک ، هر ترمینال یک گره مستقل است که ممکن است در حالت میزبان و روتر عمل نماید. به عبارت دیگر در موقع پردازش اصلی به عنوان یک میزبان عمل می کند و گره های سیار می توانند عملیات سوئیچینگ را به عنوان یک روتر انجام دهند. بنابراین نقطه پایانی و سوئیچ ها در شبکه های اقتضائی متحرک غیر قابل تشخیص هستند .
- (۲) عملیات توزیع شده: از آن جایی که هیچ ساختاری برای عملیات کنترل مرکزی شبکه وجود ندارد، کنترل و مدیریت شبکه بین ترمینال ها به صورت توزیع شده انجام می شود. گره های درگیر در شبکه های اقتضائی متحرک باید با همدیگر کار کنند و هر گره به عنوان یک تقویت کننده عمل می کند.
- (۳) مسیریابی: انواع اصلی الگوریتم های مسیریابی شبکه های اقتضائی متحرک می تواند بر مبنای خصوصیات متفاوت لایه پیوند و پروتکل های مسیریابی به صورت تک گامی و چند گامی عمل کند. شبکه تک گامی شبکه های اقتضائی متحرک از لحاظ پیاده سازی و ساختار ساده تر است و قیمت آن هم از لحاظ عملیاتی پایین تر است. موقع تحویل دادن بسته ها از یک منبع به مقصد خارج از دامنه انتقالات بی سیم مستقیم ، بسته باید توسط یک یا تعداد بیشتری گره میانی ارسال شود .
- (۴) توپولوژی پویای شبکه: از آن جایی که گره ها سیار هستند، توپولوژی شبکه ممکن است به سرعت و به صورت غیر قابل پیش بینی تغییر کند و اتصالات از میان ترمینال ها ممکن است در یک زمان تغییر کند . شبکه های اقتضائی متحرک باید ترافیک و شرایط انتشار و همچنین الگوهای حرکت گره های شبکه سیار را سازگار کند. گره های سیار در شبکه به صورت پویا مسیریابی را از میان خودشان همان طور که آنها حرکت می کنند، ایجاد می کنند و در ادامه خودشان شبکه را شکل می دهند. اگر چه، یک کاربر در یک شبکه اقتضائی متحرک ممکن است فقط درون شبکه اقتضائی متحرک عمل نکند و نیاز به شبکه ثابت داشته باشد.
- (۵) تغییر ظرفیت اتصال: طبیعت نرخ بیت خطای بالای ارتباط بی سیم ممکن است در یک شبکه اقتضائی متحرک عمیق تر باشد. یک مسیر انتها به انتها دارای تاخیرهای گوناگونی می باشد که در ظرفیت اتصال اثر گذار می باشد . کانالی که ترمینال ها را متصل می کند هدفی برای نویز، ناپدید شدن و تداخل می باشد و پهنای باند کمتری از یک شبکه سیمی دارد. در تعدادی از طرح ها، مسیر بین هر جفت از کاربران می تواند اتصالات بی سیم متعددی را بیماید.

۶) ترمینال های سبک وزن: در تعدادی حالت ها، گره های شبکه اقتضائی متحرک وسایل سیار با ظرفیت پردازش کمتر، اندازه حافظه کوچکتر، ذخیره ساری نیروی کمتری هستند این وسایل نیاز به الگوریتم های بهینه شده و مکانیسم هایی که عملیات محاسباتی و ارتباطی را بهینه می کنند دارند.

## ۱-۲-۶-۲ مزایای شبکه های اقتضائی متحرک

- ۱) خودمختار است. (مستقل از مدیریت مرکزی شبکه است و به زیرساخت نیاز ندارد).
- ۲) سرعت توسعه آن زیاد است.
- ۳) مقرون به صرفه است. (به سادگی و با صرف هزینه پایین قابل پیاده سازی است).
- ۴) قادر به خودپیکربندی و خودترمیمی است.
- ۵) مقیاس پذیر است. (خود را با اضافه شدن گره های بیشتر تطبیق می دهد).
- ۶) انعطاف پذیر است. (به عنوان مثال، دسترسی به اینترنت از نقاط مختلف موجود در محدوده تحت پوشش شبکه امکان پذیر است).
- ۷) هر یک از ایستگاه ها به عنوان یک روتر نیز ایفای نقش می کنند.
- ۸) دو ایستگاه موجود در شبکه می توانند به طور مستقل از دیگر ایستگاه ها، با یکدیگر ارتباط برقرار کرده و انتقال اطلاعات پردازند.
- ۹) ارتباط دیتای بیسیم متحرک و دستیابی به حجم انبوهی از کاربران
- ۱۰) هزینه، قابلیت حمل و قابلیت استفاده

## ۳-۶-۲ معایب شبکه های اقتضائی متحرک

صرفنظر از کاربردهای جذاب شبکه های اقتضائی متحرک، ویژگی های شبکه اقتضائی متحرک باعث محدودیت هایی در استفاده از این شبکه ها شده است، که باید بررسی شوند. یکی از چالش های بسیار مهم در این شبکه عدم وجود زیر ساخت ثابت می باشد. از بزرگترین مشکلات موجود در این شبکه می توان به موارد زیر اشاره کرد:

- ۱) مسیریابی: از آن جایی که توپولوژی شبکه به صورت مداوم در حال تغییر است، عمل مسیریابی بسته ها بین هر جفت از گره ها بسیار مشکل است. بیشتر پروتکل ها باید بر مبنای مسیریابی واکنشی به جای کنشی باشند. مسیریابی گروهی (پخش فراگیر) مشکل دیگری است، زیرا گروه ها به صورت ایستا

نیستند و به همین علت محیط تصادفی از گره ها درون شبکه ها داریم. مسیرها بین گره ها ممکن است شامل گام های متعدد باشند که پیچیده تر از ارتباطات تک گام است.

(۲) امنیت و قابل اعتماد بودن : علاوه بر قابلیت رابج ارتباط بی سیم، یک شبکه اقتضائی متحرک مسائل امنیتی مخصوصی دارد. خصوصیت عملیات توزیع شده نیاز به طرح های متفاوتی برای مدیریت کلیدی دارد. بعلاوه اتصالات بی سیم به علت دامنه انتقالات بی سیم محدود شده، طبیعت همگانی (انتشار) رسانه بی سیم (مسئله پایانه مخفی)، گم شدن بسته های متحرک، و خطاهای انتقالات داده مسائل اعتمادپذیری زیادی تولید می کنند.

(۳) کیفیت سرویس خدمات<sup>۱</sup>: فراهم کردن کیفیت های متفاوت از سطح های سرویس در یک شبکه که به صورت مداوم در حال تغییر است یک مشکل می باشد. ویژگی ذاتی تغییر، در واقع کیفیت ارتباطات در یک شبکه اقتضائی متحرک را برای پیشنهاد روی یک وسیله ثابت مشکل می کند. یک کیفیت خدمات سرویس سازگار باید برای مسیریابی و منبع برای پشتیبانی سرویس های چند رسانه ای قدیمی پیاده سازی شود.

(۴) کار در اینترنت : ارتباطات درون یک شبکه اقتضائی متحرک ، کار در اینترنت بین شبکه های ثابت و شبکه اقتضائی متحرک (در اصل بر مبنای IP) اغلب در حالات زیادی مورد انتظار است. با هم بودن پروتکل های مسیریابی در چنین وسایل سیار یک مشکل برای مدیریت تحرک است.

(۵) مصرف نیرو: برای بیشتر ترمینال های سیار سبک وزن، عملیات های مبتنی بر ارتباط، باید برای مصرف انرژی بهینه شوند. نگهداری نیرو و مسیریابی که مراقب نیرو باشد، باید در نظر گرفته شود.

از مشکلات و محدودیت های دیگر موجود در شبکه های اقتضائی متحرک می توان موارد زیر را نام برد.

- (۱) هر گره باید دارای کارایی کامل باشد.
- (۲) برای قابلیت اطمینان به تعداد کافی از گره های در دسترس نیاز دارد. در نتیجه شبکه های پراکنده می توانند مشکلاتی را به همراه داشته باشند.
- (۳) در شبکه های بزرگ ممکن است تاخیر زمانی زیادی داشته باشد.
- (۴) دارای انرژی محدود است. چون گره ها، انرژی خود را از باتری ها بدست می آورند. ( طول کم شارژ باتری ابزار متحرک )

- ۵) امنیت آن محدود است.
- ۶) خطاهای ناشی از انتقال و در نتیجه هدر رفتن زیاد بسته ها.
- ۷) حضور لینکهای با ظرفیت متغیر.
- ۸) قطع و وصل شدن های زیاد و مداوم
- ۹) پهنای باند محدود و طبیعت پخش فراگیر ارتباطات.
- ۱۰) مسیر ها و توپولوژی های متغیر و پویا
- ۱۱) ظرفیت ها و قابلیت های محدود گره ها.
- ۱۲) نیاز به برنامه های کاربردی جدید ( لایه ی Application )
- ۱۳) کنترل میزان تراکم و جریان داده ها ( لایه ی Transport )
- ۱۴) روش های آدرس دهی و مسیریابی جدید ( لایه ی Network )
- ۱۵) تغییر در وسایل و ابزار آلات اتصالی ( لایه ی Link )
- ۱۶) خطاهای انتقال ( لایه ی Physical )

## ۲-۶-۴ کاربردهای شبکه های اقتضائی متحرک

شبکه های اقتضائی معمولا در مواقعی که نیاز به پیاده سازی سریع یک شبکه ارتباطی است و زیرساختی در دسترس نبوده و ایجاد و احداث زیرساخت نیز مقرون به صرفه نباشد، کاربرد دارند. به عنوان نمونه با مجهز کردن یک میدان جنگ به دستگاه هایی که از حسگر لرزش، سیستم GPS و حسگر مغناطیسی برخوردارند، می توان عبور و مرور خودروها در محل را کنترل نمود. هر یک از ابزارها پس از حس کردن موقعیت جغرافیایی خود با ارسال یک موج رادیویی، ابزارهایی را که در محدوده ای به وسعت ۳۰ متر از آن قرار دارند را شناسایی کرده و با آن ارتباط برقرار می کند. از جمله کاربران شبکه های اقتضائی می توان به پلی استیشن سونی اشاره کرد که از اتصالات اقتضائی برای ایجاد شبکه بی سیم بین چند بازیکن (که همگی در یک بازی شرکت می کنند) اشاره کرد. پس از پایان بازی، اتصال بی سیم بین کاربران قطع می شود.

شبکه های اجتماعی جدید با استفاده از ترکیبی از محاسبات رایانه ای و ارتباطات مخابراتی ایجاد می شوند. آگاهی از مکان، محاسبات نقطه به نقطه و فناوری های شبکه بی سیم طراحی شبکه های اقتضائی را برای دستگاه های متحرک که مهم ترین ابزار ایجاد شبکه های اجتماعی هستند، امکان پذیر ساخته است. شبکه های اقتضائی متحرک می تواند هرجایی که کوچک است و زیر ساختار ارتباطی وجود ندارد یا زیر ساختار ارتباطی گران



است و یا استفاده از زیر ساخت دشوار است، مفید باشد. شبکه بندی شبکه اقتضائی اجازه می دهد که وسایل به راحتی به شبکه اضافه بشوند یا از شبکه برداشته شوند.

از جمله این کاربردها می توان به موارد زیر اشاره کرد:

(۱) استفاده در شبکه های شخصی<sup>۱</sup>

این نوع شبکه در برگیرنده سیستم های بی سیم که دارای برد و قدرت پایین هستند، می باشد. این نوع شبکه ها معمولاً بین افراد و یا در یک دفتر کار و مکان های مشابه ایجاد می گردد.

(۲) حفاظت از محیط زیست

زیست شناسان با استفاده از گردن آویزهایی که به حسگرهای مکان، دما و دیگر حس گرها مجهز هستند کیفیت زندگی حیوانات در خطر انقراض را کنترل می نمایند. زمانی که حیوان دارای گردن آویز، حرکت می کند اطلاعات مربوط به مسیر حرکت او از حسگرهای مرتبط جمع آوری می شوند و سپس توسط زیست شناسان مورد پردازش قرار می گیرند.

(۳) تلفن های سلولی، کامپیوترهای کیفی، ساعت های مچی

(۴) سربازها و تانکها و هواپیماها

(۵) در نبردهایی که کنترل از راه دور صورت می گیرد

(۶) برای ارتباطات و کاربردهای نظامی : امروزه تجهیزات نظامی جدید شامل تعداد زیادی از تجهیزات کامپیوتری می باشد.

(۷) توانایی باقی ماندن در میدان منازعه

(۸) محیط های غیرنظامی و صنعتی

(۹) شبکه تاکسی رانی

(۱۰) اتاق های ملاقات

(۱۱) میادین یا ورزشگاه های ورزشی

(۱۲) قایق ها، هواپیماهای کوچک

(۱۳) به اشتراک گذاری داده ها توسط شرکت کنندگان در یک کنفرانس - جلسات

(۱۴) عملکردهای فوری، محیط های علمی

در محیط های علمی و تحقیقاتی در برخی از مناطق که دانشمندان برای نخستین بار اقدام به بررسی می کنند، به علت عدم وجود زیرساختار، شبکه اقتضائی بسیار مفید می باشد.

(۱۵) عملیات جستجو، نجات، اطفاء حریق، عملیات پلیسی

(۱۶) موقعیت های امدادی برای حادثه های بد و فوری (عملیات اورژانسی)

(۱۷) برای ترمیم و بدست آوردن اطلاعات در حوادث بد و غیرمترقبه مانند وقوع بلایای طبیعی چون سیل و

طوفان و زلزله

## ۲-۵ امنیت شبکه های اقتضائی متحرک

شبکه های اقتضائی متحرک نیز مانند بسیاری از شبکه های بی سیم و سیمی برای انجام و کارکرد صحیح اعمال شبکه که در اینجا شامل مسیریابی، جلورانی بسته های داده، نگهداری و به روز رسانی اطلاعات مسیریابی است، به امنیت نیازمند هستند. در واقع امنیت شرط لازم برای عملکرد درست اعمال شبکه است و بدون نبود آن تضمینی برای انجام صحیح این اعمال وجود ندارد و مهاجمان به راحتی می توانند یکپارچگی شبکه را بر هم بزنند. سیاستی که در این راستا تدبیر می شود آن است که اعتماد کامل به گره های شبکه برای انجام اعمال حیاتی شبکه کاری عبث و بیهوده است و این رابطه اعتماد تنها در برخی از سناریوهای شبکه اقتضائی متحرک قابل فرض است. مثلاً در یک شبکه اقتضائی متحرک که گره های آن سربازان یک گروهان باشند می توان از قبل، یعنی پیش از شروع عملیات، کلیدهای متقارن مشترک و یا کلیدهای عمومی افراد (بسته به نوع رمزنگاری متقارن یا نامتقارن) را با یکدیگر مبادله کرد. ولی مشکلات و محدودیتهای دیگری همچنان باقی می ماند. از جمله اینکه چنین شبکه ای نمی تواند امنیت را برای قرارگیری افزایشی تامین کند. چرا که گره های جدیدی که می خواهند در شبکه قرار گیرند باید به نوعی خود را به گره های دیگر معرفی کنند و احراز اصالت متقابل برای همه آنها بتواند، صورت بگیرد.

گره های شبکه اقتضائی متحرک برای انجام مدیریت کلید به یک محیط مدیریت شده نیاز دارند. در واقع باید یک یا چند مرکز معتمد وجود داشته باشند تا گره های تازه وارد را در شبکه ثبت کنند و گره های مخرب را از شبکه خط بزنند و بدین ترتیب امنیت شبکه مورد نظر را بر اساس گره های سالم موجود تامین کنند، چرا که گره های مخرب در لیست ابطال قرار گرفته اند. منظور از کارکرد صحیح اعمال شبکه این است که هر گره ای از شبکه به وظایف خود مبنی بر جلورانی بسته ها و مسیریابی به درستی عمل کند و در این عملیاتها به خوبی با دیگر گره ها همکاری و مشارکت کند. یعنی اینکه در نهایت اعمال شبکه بین گره ها به صورت منصفانه تقسیم شود. با

توجه به ماهیت ذاتی شبکه های اقتضائی متحرک بسادگی می توان چنین برداشت کرد که عملکرد شبکه شدیداً وابسته به رفتار گره های شبکه می باشد. یعنی اگر گره ای وظایفش را به درستی انجام ندهد، بازده عملکرد شبکه به شدت افت می کند و تبادل اطلاعات حیاتی ممکن است به خطر افتد. بر این اساس در برخی از مدل های پیشنهادی برای برقراری امنیت از منطق اکثریت استفاده می کنند و رفتار ناصحیح گره ها را بر اساس سابقه اعمال آنها بررسی می کنند و اگر این سابقه از یک حد آستانه مربوط به متوسط اعمال بدتر باشد رفتار گره مخرب تشخیص داده می شود. البته این تصمیم گیرها تا حدی نسبی اند و هرگز به طور مطلق نمی توان تعیین کرد که هر رفتاری که از گره ای سر می زند صحیح است یا ناصحیح. برای پیدا کردن گره خرابکار به انجام اعمالی چون ردیابی، نگهداری و دیده بانی نیاز است که خود محتاج پردازش ارتباطاتی بالا می باشد که هم انرژی می طلبد و هم پهنای باند و حافظه. در نتیجه در شبکه های بی سیم همانند شبکه های اقتضائی نمی توان از پروتکل های شبکه همانند BGP استفاده کرد. هم از جهت محدودیت پردازش ارتباطاتی و هم از این جهت که توپولوژی شبکه دائماً در حال تغییر است.

## ۲-۵-۱ انواع حملات بر روی شبکه های اقتضائی

حملات انجام شده بر روی شبکه های اقتضائی را می توان از چند جنبه دسته بندی کرد. در اینجا ابتدا یک دسته بندی کلاسیک از حملات ارائه شده است.

حملات فعال که در آنها گره بدرفتار برای اجرای تهدید خودش باید هزینه انرژی آن را پردازد. چنین گره ای اصطلاحاً گره مخرب یا بداندیش نامیده میشود. هدف از انجام این حمله از هم گسستگی شبکه یا ضرر رساندن به گره های دیگر است.

حملات غیرفعال که در آنها گره بدرفتار به قصد ذخیره انرژی از همکاری امتناع می کند. چنین گره ای گره خودخواه نامیده می شود. هدف از انجام این حمله کاهش عملکرد شبکه یا تقسیم شبکه با شرکت نکردن در عملیات ها است. از دیدگاهی دیگر می توان حملات را به سه بخش تقسیم کرد که هر کدام از این بخشها را می توان جزئی از حمله فعال ذکر شده در بالا نیز محسوب کرد. در واقع حمله غیرفعال می تواند به طور غیرمستقیم بر روی عملکرد شبکه تاثیر بگذارد لذا آن را به عنوان یک مورد خاص هم می توان در نظر گرفت. در عمل همواره ترکیبی از حمله فعال به همراه غیرفعال وجود دارد. حمله به قصد تغییر بر روی پروتکل های فعلی قابل اعمال است چرا که پروتکل های فعلی هیچ حفاظتی در برابر یکپارچگی اطلاعات ندارند لذا براحتی قابل تغییرند. در نتیجه گره خرابکار می تواند یکپارچگی محاسبات مسیریابی را با تغییر بر هم بزند و بدین طریق بسته های

اطلاعات صحیح را دور بریزد و پروسه را به کشف مسیر نادرست هدایت کند و یا اینکه مسیر ترافیک را طولانی کند و یا اینکه باعث ازدیاد ترافیک در یک مسیر خاص شود. حمله به قصد جعل هویت به این صورت است که گره خرابکار اصالت خود را به گره دیگری تغییر می دهد و از آنجا که در پروتکل های فعلی بسته ها احراز اصالت نمی شوند، مهاجم با هویت نادرست شناخته می شود. به این حمله در امنیت شبکه اصطلاحاً Spoofing گفته می شود که در اینجا مهاجم حتی می تواند تصویر توپولوژی شبکه را تغییر دهد و یا در اطلاعات مسیریابی حلقه تکرار بینهایت ایجاد کند. حمله به قصد جعل پیام برای تولید پیامهای مسیریابی غلط توسط گره مخرب و حذف گره همسایه با ارسال خطای مسیریابی جعلی است. متأسفانه این حملات به سختی قابل تشخیص اند چرا که جاعل پیام را نمی توان براحتی شناسایی کرد و مهاجم براحتی می تواند قسمتهای مختلف پیام را به نفع خود تنظیم کند و بعد آنها را در میان شبکه پخش کند.

از انواع دیگر حملات می توان حمله DoS را نام برد که مهاجم بسته صحیح داده را به قصد گسستن مسیریابی در مسیر غلط هدایت می کند. از دیگر انواع این حمله می توان از حمله مصرف منابع نام برد که در آن حمله کننده برای اشغال پهنای باند کانال، توان محاسباتی، یا حافظه گره ها به شبکه داده بی مورد تزریق می کند. در حمله سیاه چاله مهاجم با انتشار اخبار دروغین مسیریابی برای کوتاهترین مسیر، ترافیک شبکه را به طرف خود جذب می کند و سپس آن را دور میریزد. مدل پیشرفته تر حمله سیاه چاله حمله Grey-hole است که در آن مهاجم تنها بسته های داده را دور می ریزد، ولی بسته های مسیریابی را ارسال می کند تا مسیر ساختگی خود را پابرجا نگاه دارد! در حمله انحراف بلاعوض مهاجم با افزودن گره های مجازی به اطلاعات مسیریابی مسیر را بلندتر نشان میدهد. در حمله سریع مهاجم اخبار نادرست درخواست مسیر را به سرعت در سراسر شبکه پخش میکند تا گره ها به علت تکرار پیام درخواست صحیح مسیریابی را دور بریزند. حمله لانه کرمی به عنوان یک حمله ماهرانه تلقی می شود که در آن دو مهاجم فعال با ایجاد یک تونل ارتباط خصوصی مجازی جریان عادی حرکت پیامها را اتصال کوتاه می کنند و با این روش می توانند دو گره غیرمجاور را با هم همسایه کنند و یا از پروتکل کشف مسیر جلوگیری کنند. متأسفانه بسیاری از پروتکل های مسیریابی مانند :

DSR، AODV، OLSR، و TBRPF به این حمله آسیب پذیرند.

## ۲-۵-۶-۲ اهداف امنیتی در شبکه های اقتضائی متحرک

ایجاد امنیت برای شبکه های اقتضائی متحرک را می توان در قالب دستیابی به پنج هدف دسته بندی کرد:

(۱) قابلیت دسترسی<sup>۱</sup>

(۲) ایجاد اطمینان<sup>۲</sup>

(۳) تغییر نیافتن داده ارسالی در طول مسیر<sup>۳</sup>

(۴) اصالت سنجی<sup>۴</sup>

(۵) انکارناپذیری<sup>۵</sup>

قابلیت دسترسی: در شبکه به معنای قابل دسترس بودن تمام نودها در صورت نیاز به برقراری ارتباط می باشد (اگر نود مورد نظر در رنج رادیویی شبکه باشد). داشتن این مشخصه در شبکه به این معنا است که، حمله کننده، چه از خارج شبکه و چه از داخل شبکه، نمی تواند مانع برقراری ارتباط با یک نود شود. در تعریف دیگر می توان گفت شبکه با داشتن این خصیصه تحت تاثیر حمله DOS قرار نمی گیرد.

ایجاد اطمینان: این مشخصه زمانی در شبکه بوجود می آید که مطمئن باشیم هر آنچه در شبکه منتقل شده در دسترس نودهای غیر مجاز قرار نگرفته است. به دلیل بعضی کاربردهای خاص نظامی داده منتقل شده در شبکه های اقتضائی متحرک نباید به آسانی در دسترس قرار گیرد. بجز محتوای بسته های داده منتقل شده، اطلاعات مربوط به مسیریابی نیز در بعضی از کاربردها نباید در دسترس نودهای متخاصم قرار بگیرد.

تغییر نیافتن داده ارسالی در طول مسیر: وجود این مشخصه در شبکه دریافت کننده بسته را از اینکه بسته در حین عبور از شبکه دچار تغییر نشده مطمئن می نماید. این تغییر می تواند بدلیل نارسایی لینک رادیویی بوجود آمده باشد یا به دلیل عملکرد یک نود متخاصم.

اصالت سنجی: این مشخصه باعث می شود تا هر نود در شبکه بتواند از هویت نود مقابلش اطمینان حاصل نماید. بدون اصالت سنجی نود متخاصم می تواند هویت نود دیگری را در شبکه جعل نماید و به اطلاعاتی که در حالت عادی برای آن نود قابل دسترسی نیست دسترسی پیدا نماید، یا اطلاعات نودهای دیگر را دستکاری نموده به جای آنها ارسال نماید.

انکارناپذیری: وجود این مشخصه در شبکه به آن معنا است که هر نودی که در شبکه اقدام به ارسال داده می نماید نتواند ارسال آن داده را انکار نماید. داشتن این خاصیت به شبکه امکان می دهد تا نودهایی را که عملکرد

- 
- 1 - Availability
  - 2- Confidentiality
  - 3- Integrity
  - 4- Authentication
  - 5- non-repudiation

نامناسب و در شبکه دارند را شناسایی نماید برای مثال اگر نود A از نود B بسته ای دریافت نماید که تشخیص دهد نود B قصد حمله به شبکه را دارا است، می تواند ادعای خود را به همراه بسته ارسالی از جانب B همراه نموده، برای نودهای دیگر شبکه بفرستد. به علت اینکه نود B نمی تواند ارسال بسته را تکذیب نماید و نود B از جانب کل شبکه به عنوان یک نود با عملکرد نامناسب شناخته شود.

## ۲-۶-۵-۳ چالش های امنیتی در شبکه های اقتضائی متحرک

- (۱) نبود زیرساخت یا کنترل مرکزی، مدیریت شبکه را مشکل می کند.
- (۲) به دلیل توپولوژی پویای شبکه، نیازمند مسیریابی پیشرفته و امن است.
- (۳) با توجه به امکان عدم همکاری گره ها، مکانیزم های مسیریابی آسیب پذیر می باشند.
- (۴) از آنجایی که ارتباطات از طریق امواج رادیویی هستند، جلوگیری از استراق سمع مشکل است.

## ۲-۷ جمع بندی

شبکه های اقتضائی موبایل در واقع آینده شبکه های بی سیم می باشند به دلیل اینکه آنها ارزان، ساده، انعطاف پذیر و استفاده آسانی دارند. ما در جهانی زندگی می کنیم که شبکه ها در آن پیوسته تغییر می کنند و توپولوژی خودشان را برای اتصال نودهای جدید تغییر می دهند. با توجه به نودهای متحرک در شبکه های اقتضائی متحرک (موبایل) و ویژگی های ساختاری آن می توان گفت برای مکان هایی با توپولوژی پویا که فاقد زیرساخت ثابت بوده یا اینکه زیرساخت های موجود بسیار گران قیمت بوده و استفاده از آنها راحت نیست، کاربران سیار بی سیم می توانند از طریق شبکه های اقتضائی متحرک با یکدیگر ارتباط برقرار کنند. هرچند به دلیل خصوصیات ساختاری و معایبی که این شبکه دارد استفاده از آنها با محدودیت مواجه شده است. یکی از مهمترین مواردی که در این گونه شبکه ها مورد بحث و توجه قرار می گیرد، مبحث مسیریابی و امنیت پیرامون آن می باشد. هرچند تاکنون الگوریتم های مسیریابی مختلفی با ارائه راهکارهای امنیتی آن ارائه شده، ولی همچنان الگوریتم های مسیریابی شبکه های موبایل مبحث مهمی برای تحقیق و توسعه می باشد. بنابراین در فصل های بعدی تا آنجا که ممکن است در مورد مسیریابی و انواع مسیریابی صحبت خواهیم کرد.

## فصل سوم

### مسیریابی

### ۳-۱ مقدمه

در شبکه های کوچک و در نقاطی که انتقال اطلاعات معمولاً مستقیم است، مسیریابی چندان جدی گرفته نمی شود. اما هنگامی که شبکه ها از حالت های ایستگاه های کاری خارج می شوند و کمی پیچیده تر می شوند، در این حالت، مسیریابی و انتخاب مسیر بهینه برای ارسال بسته های اطلاعاتی، به یک امر مهم بدل می شود. مسیریابی فرآیندی مبتنی بر یک سری قواعد منطقی و سیاست هاست که پیچیدگی آن به سطوح و لایه ی امنیت، امکان پشتیبانی همزمان از دو یا سه پروتکل و پیچیدگی ساختار و توپولوژی شبکه را می دهد. انتقال داده ها از یک شبکه به شبکه دیگر وقتی که تنها یک مسیر واحد بین آن دو شبکه وجود دارد، ساده ترین فرآیند مسیریابی است، اما زمانی که بین دو شبکه چندین مسیر وجود دارد، مکانیزم پیدا کردن بهترین مسیر و همچنین اعمال معیارهای بهینگی مسیر، به الگوریتم های پویا نیاز دارد. بدیهی است که الگوریتمی بهتر است که صحت عملکرد بالایی داشته باشد و در عین حال ساده باشد، اما چه الگوریتمی قابلیت اتکای خوبی دارد؟ الگوریتمی مناسب است که در گذشت زمان، با تغییر نرم افزارها و سخت افزارهای شبکه و تغییر پروتکل ها، همچنان مسیریابی درستی ارائه دهد. همچنین مهم است که بعد از یک مدت زمان خاص، الگوریتم مسیریابی به حالتی پایدار برسد و همزمان با آن، مسیریابی بهینه ای داشته باشد و در ارسال بسته ها عدالت را رعایت کند. بدین منظور در این فصل به انواع الگوریتم های مسیریابی می پردازیم.

### ۳-۲ الگوریتم های مسیریابی

وظیفه اصلی لایه شبکه، هدایت بسته ها از ماشین منبع به ماشین مقصد است. الگوریتم مسیریابی بخشی از نرم افزار لایه شبکه است که تعیین می کند بسته ورودی باید به کدام خط خروجی منتقل شود. اگر زیر شبکه از دیتاگرام استفاده کند، این تصمیم گیری دوباره باید برای هر بسته ورودی تکرار شود، چون تا آن موقع امکان دارد بهترین مسیر، تغییر کند. اگر زیر شبکه از مدارهای مجازی استفاده کند، تصمیمات مسیریابی وقتی اتخاذ می شوند که مدار مجازی جدیدی استفاده گردد. از آن پس، بسته های داده ها فقط از مسیر ایجاد شده قبلی منتقل می شوند. حالت مدار مجازی گاهی مسیریابی تماس نام دارد، زیرا مسیر در طول مدت تماس کاربر باقی می ماند (مثل کار کردن با پایانه یا انتقال فایل). فرآیند مسیریابی و فرآیند هدایت دو مقوله جدا از هم هستند. هر مسیریاب دارای دو پروسه می باشد، یکی به محض وارد شدن بسته ها، آن ها را پردازش کرده و از طریق جدول مسیریابی، خط خروجی مناسب انتخاب می گردد که این عمل هدایت می باشد و پروسه دیگری وظیفه



بر کردن و بروز کردن محتویات جدول مسیریابی را دارد که این توسط الگوریتم های مسیریابی انجام می گردد و فرایند مسیریابی نام دارد . الگوریتم های مسیریابی باید دارای ویژگی هایی باشند ، از جمله :

- (۱) صحت عملکرد
- (۲) سادگی
- (۳) قابلیت اطمینان
- (۴) پایداری
- (۵) عدالت
- (۶) بهینگی

بدیهی است که الگوریتمی بهتر است که صحت عملکرد بالایی داشته باشد و در عین حال ساده باشد . الگوریتمی مناسب است که در گذشت زمان، با تغییر نرم افزارها و سخت افزارهای شبکه و تغییر پروتکل ها، همچنان مسیریابی درستی ارائه دهد. همچنین مهم است که بعد از یک مدت زمان خاص، الگوریتم مسیریابی به حالتی پایدار برسد و همزمان با آن، مسیریابی بهینه ای داشته باشد و در ارسال بسته ها عدالت را رعایت نماید.

### ۳-۲-۱ دیدگاه های الگوریتم های مسیریابی

دو دیدگاه در مورد الگوریتم های مسیریابی وجود دارد که عبارتند از:

الف) دیدگاه روش تصمیم گیری و میزان هوشمندی الگوریتم

ب) دیدگاه چگونگی جمع آوری و پردازش اطلاعات زیرساخت ارتباطی شبکه

با دیدگاه اول الگوریتم های مسیریابی را می توان به دو دسته " ایستا " و " پویا " تقسیم بندی کرد.

### ۳-۲-۱-۱ مسیریابی به صورت ایستا

در الگوریتم های ایستا هیچ اعتنایی به شرایط توپولوژی و ترافیک لحظه ای شبکه نمی شود . معمولاً در این الگوریتم ها برای هدایت یک بسته ، هر مسیریاب از جداول استفاده می کند که در هنگام برپایی شبکه تنظیم شده و در طول زمان ثابت است . در هنگام وقوع هرگونه تغییر در توپولوژی زیرساخت شبکه ، این جداول باید توسط مسئول شبکه بصورت دستی مجدداً تنظیم شود . مدیر شبکه تصمیم می گیرد که زمانی که یک مسیریاب بسته هایی را که به مقصد یک شبکه معین تولید شده اند دریافت می کند، چه کاری باید انجام دهد و بنابر آن تصمیم اطلاعاتی را که نتیجه مورد نظر را به وجود می آورد به جدول مسیریابی به طور دستی اضافه می کند . اگرچه این الگوریتم ها بسیار سریعند ولی چون ترافیک لحظه ای شبکه متغیر است ، نمی توانند بهترین مسیرها را انتخاب

نمایند و هرگونه تغییر در توپولوژی زیرساخت ارتباطی شبکه، یک مشکل عمده و جدی ایجاد خواهد کرد. این روش در شبکه های نسبتاً کوچک که دارای تعداد کمی مسیریاب هستند عملی می باشد و در شبکه های بزرگ پیکربندی دستی بسیار سنگین و پیچیده می باشد و مسیریابها قادر نخواهند بود بنابه شرایط شبکه جداول خود را اصلاح کنند.

### ۳-۲-۱-۲ مسیریابی به صورت دینامیک یا پویا

در الگوریتم های پویا، مسیریابی براساس آخرین وضعیت توپولوژی و ترافیک شبکه انجام می شود. جداول مسیریابی در این نوع الگوریتم ها هر  $t$  ثانیه یکبار به هنگام می شود. این الگوریتم ها براساس وضعیت فعلی شبکه تصمیم گیری می نمایند ولی ممکن است پیچیدگی این الگوریتمها به قدری زیاد باشد که زمان تصمیم گیری برای انتخاب بهترین مسیر، طولانی شده و منجر به تاخیرهای بحرانی شده و نهایتاً به ازدحام می انجامد، به همین دلیل در مسیریاب های سریع از تکنیک های چند پردازنده ای و پردازش موازی استفاده می شود. مسیریاب های پویا انعطاف پذیرتر از مسیریاب های ایستا هستند. به نسبت مسیریاب های ایستا، مسیریاب های پویا توانایی غلبه بر ترافیک شبکه ها را دارا بوده و با استفاده از مسیرهای مختلف، بسته ها را به جلو پیش می برند. در کل عملکرد مسیریابهای پویا بهتر از مسیریاب های ایستا می باشد.

از دیدگاه دوم الگوریتمهای مسیریابی به دو دسته "سراسری یا متمرکز" و "غیرمتمرکز" تقسیم می شود. در الگوریتم های سراسری یا متمرکز هر مسیریاب باید اطلاعات کاملی از زیرساخت ارتباطی شبکه داشته باشد. یعنی هر مسیریاب باید تمامی مسیریاب های دیگر، ارتباطات بین آنها و هزینه هر خط را دقیقاً شناسایی نماید. سپس با جمع آوری این اطلاعات ساختمان داده مربوط به گراف زیرساخت شبکه را تشکیل بدهد، در چنین شرایطی برای یافتن بهترین مسیر بین هر دو مسیریاب، از الگوریتمهای کوتاهترین مسیر نظیر الگوریتم دایجکسترا استفاده می شود. به چنین الگوریتمهایی که برای مسیریابی ها اطلاعات کاملی از زیر ساخت شبکه و هزینه ارتباط بین هر دو مسیریاب نیازمندند، اختصاراً الگوریتم های حالت لینک یا حالت پیوند گفته می شود و در مسیریاب های مدرن و جدید از آن استفاده می شود.

در الگوریتم های غیرمتمرکز، مسیریاب اطلاعات کاملی از زیرساخت شبکه ندارد بلکه فقط قادر است هزینه ی ارتباط با مسیریاب هایی که بطور مستقیم و فیزیکی با آنها در ارتباط است محاسبه و ارزیابی نماید. سپس در فواصل زمانی منظم، هر مسیریاب جدول مسیریابی خود را برای مسیریابهای مجاور، ارسال می نماید. مسیریاب با دریافت این جداول و مقادیری که خودش مستقیماً اندازه گیری کرده، بایک الگوریتم بسیار ساده جدول

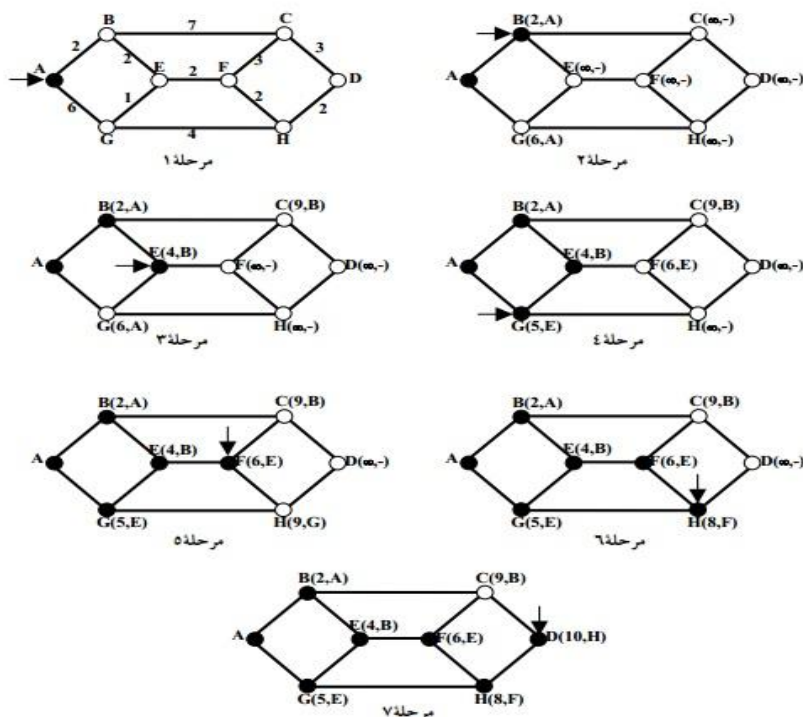
خودش رابه هنگام می نماید و برای هدایت هر بسته ، از آن استفاده می کند . در این الگوریتم ها برای مسیریابی هر بسته ، فقط یک جستجو در جدول مسیریابی کافی است و در نتیجه پیچیدگی زمانی بسیار مناسبی دارد چرا که درگیر اجرای الگوریتم های وقت گیری شبیه دایجکسترا نخواهند شد . به این نوع الگوریتم ها به اختصار الگوریتم های بردار فاصله گفته می شود . در ادامه در مورد این روش ها مفصل تر بحث خواهیم نمود .

### ۳-۳ اصل بهینگی

توجه به این اصل مهم است که صرف نظر از توپولوژی شبکه و ترافیک ، می توان حکمی کلی راجع به مسیرهای بهینه ارائه کرد . این حکم به عنوان اصل بهینگی شناخته می شود . این اصل بیان می کند که اگر مسیریاب A بر روی مسیر بهینه بین مسیریاب B تا مسیریاب C واقع شده باشد بنابراین مسیر بهینه از A تا C نیز بر روی همان مسیر خواهد بود .

### ۳-۴ مسیر یابی کوتاه ترین مسیر

مطالعه الگوریتمهای مسیریابی را با تکنیکی که به طور گسترده به شکل های مختلفی به کار می رود شروع می کنیم ، زیرا الگوریتم ساده ای است و درک آن آسان است . ایده ، ساختن گرافی از زیر شبکه است ، به طوری که هر گره گراف ، نشان دهنده مسیریاب است و هریال نشان دهنده خط ارتباطی است ( که اغلب پیوند نام دارد ) . برای انتخاب مسیری بین دو مسیریاب معین ، الگوریتم ، کوتاهترین مسیر بین آنها را در گراف می یابد . یک راه اندازه گیری طول مسیر ، تعداد جهش است ، فاصله جغرافیایی به کیلومتر است ، هریال می تواند به میانگین تاخیر صف بندی و انتقال برای بعضی از بسته های آزمایشی برچسب گذاری گردد . در حالت کلی ، برچسب های یال ها باید به صورت تابعی از فاصله ، پهنای باند ، میانگین ترافیک هزینه ارتباط ، میانگین طول صف تاخیر اندازه گیری شده و سایر عوامل محاسبه شود . با تغییر تابع وزنی ، الگوریتم ، کوتاهترین مسیر وزن دار را براساس هریک از معیارهای فوق یا ترکیبی از آنها محاسبه می کند . الگوریتم های متعددی برای محاسبه کوتاهترین مسیر بین گره های گراف شناسایی شده اند که یکی از این الگوریتم ها به دایجکسترا ۱۹۹۵ نسبت داده می شود .



شکل ۳-۱ مسیریابی کوتاهترین مسیر با الگوریتم دایجکسترا

### ۳-۵ الگوریتم غرق کردن (سیل آسا)<sup>۱</sup>

در این روش ، هر بسته ورودی که به یک مسیریاب می رسد ، از تمام کانال های خروجی مسیریاب خارج می شود ، بدین ترتیب تعداد زیادی بسته تکراری وجود خواهد داشت و عملاً میزان آن بی نهایت خواهد بود . بنابراین برای خاتمه این تعداد بسته ها راهکاری باید ارائه کرد . راهکارهای پیشنهادی برای این روش ، استفاده از یک شمارنده گام می باشد . بدین صورت که در سرآیند هر بسته یک شمارنده بگذاریم و در هر گام یک شماره از آن کم کنیم تا به صفر برسد و بسته حذف شود . در این صورت مبداء باید طول شبکه را بداند و در بدترین حالت ، طول شبکه را طولانی ترین فاصله در نظر بگیرد . راهکار دیگری که حالت نیمه منطقی می باشد ، مسیریاب بسته را به تمام کانال های خروجی نمی فرستد ، بلکه به کانال هایی می فرستد که احتمال رسیدن آن ها به مقصد وجود دارند ، در این صورت اگر بسته ای به سمت غرب بخواند برود ، نبایستی از کانال های شرقی مسیریاب استفاده نمود . مگر آن که مسیریاب از ساختار شبکه مطلع باشد و بداند این کانال ها به کجا منتهی می شوند . الگوریتم های سیل آسا به جز چند مورد خاص ، از جمله سیستم های توزیعی که عملکردهای موازی در آن ها نیاز است ، کاربرد علمی دیگری ندارد . الگوریتم غرق کردن، در اغلب کاربردها عملی نیست، اما کاربردهایی دارد به عنوان مثال در کاربردهای نظامی ، که لازم است در هر لحظه بیت هایی برای بسیاری از مسیر

یاب ها ارسال شود، الگوریتم غرق کردن می تواند استفاده شود. کاربرد دیگری از غرق کردن، همواره کوتاهترین مسیر را انتخاب می کند، زیرا تمام مسیرهای ممکن را به طور موازی آزمایش می کند در نتیجه هیچ الگوریتم دیگری مثل آن نمی تواند تاخیر کمتری ایجاد نماید البته اگر سربار حاصل از خود فرایند غرق کردن را نادیده بگیریم.

### ۳-۶ مسیریابی بردار فاصله<sup>۱</sup>

الگوریتم مسیریابی بردار فاصله به اسامی دیگر نیز خوانده می شود. از جمله الگوریتم مسیریابی بلمن<sup>۲</sup> - فورد و الگوریتم فورد - فوکرسون که نامگذاری آنها از نام مخترعین آنها بلمن، ۱۹۷۵ فورد و فوکرسون، ۱۹۶۲ اقتباس شده است. این الگوریتم مسیریابی آرپانت اولیه بود و تحت نام RIP<sup>۲</sup> در اینترنت مورد استفاده قرار گرفت. در این روش، مسیر یاب ها در خود جدولی (بردار) ذخیره می کنند با عنوان بردار فاصله که در آن بهترین فاصله تا هر مسیر یاب دیگر در شبکه را ذخیره می کنند. در این صورت، تصمیم گیری بهتری هنگام مسیریابی اتخاذ می شود. این جدول ها با اطلاعات مسیر یاب های همسایه به روز می شود. هر یک از عناصر این جدول ها یک درایه دوبخشی دارند که یکی از آنها نشانگر خط خروجی مناسب برای رسیدن به مسیر یاب مورد نظر و دیگری تخمین فاصله زمانی تا آن مسیر یاب است. این فاصله زمانی ممکن است تعداد جهش ها، زمان تاخیر به میلی ثانیه، بسته هایی که در مسیر در صف قرار گرفته اند یا چیزهایی مشابه آن ها باشند.

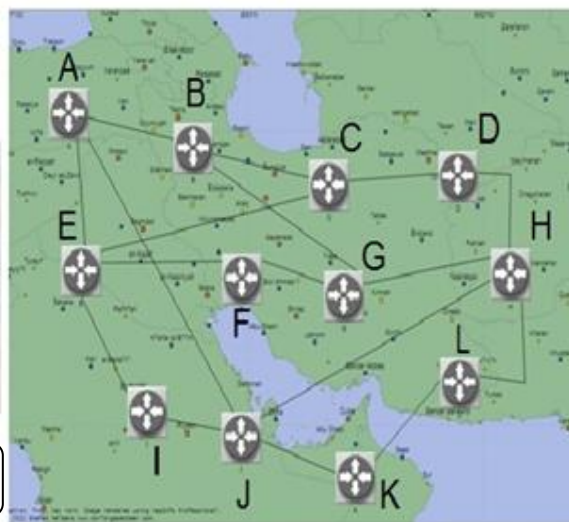
خط	هزینه تقریبی
A	8
B	20
C	28
D	20
E	17
F	30
G	18
H	12
I	10
J	0
K	6
L	15

A	I	H	K
0	24	20	21
12	36	31	28
25	18	19	36
40	27	8	24
14	7	30	22
23	20	19	40
18	31	6	31
17	20	0	19
21	0	14	22
9	11	7	10
24	22	22	0
29	33	9	9

جدول مسیریابی جدید در J

جدول دریافتی از همسایگان J



(الف)

(ب)

شکل ۳-۲ (الف) یک زیر شبکه، (ب) جداول دریافتی از همسایگان J و جدول مسیریابی جدید در J

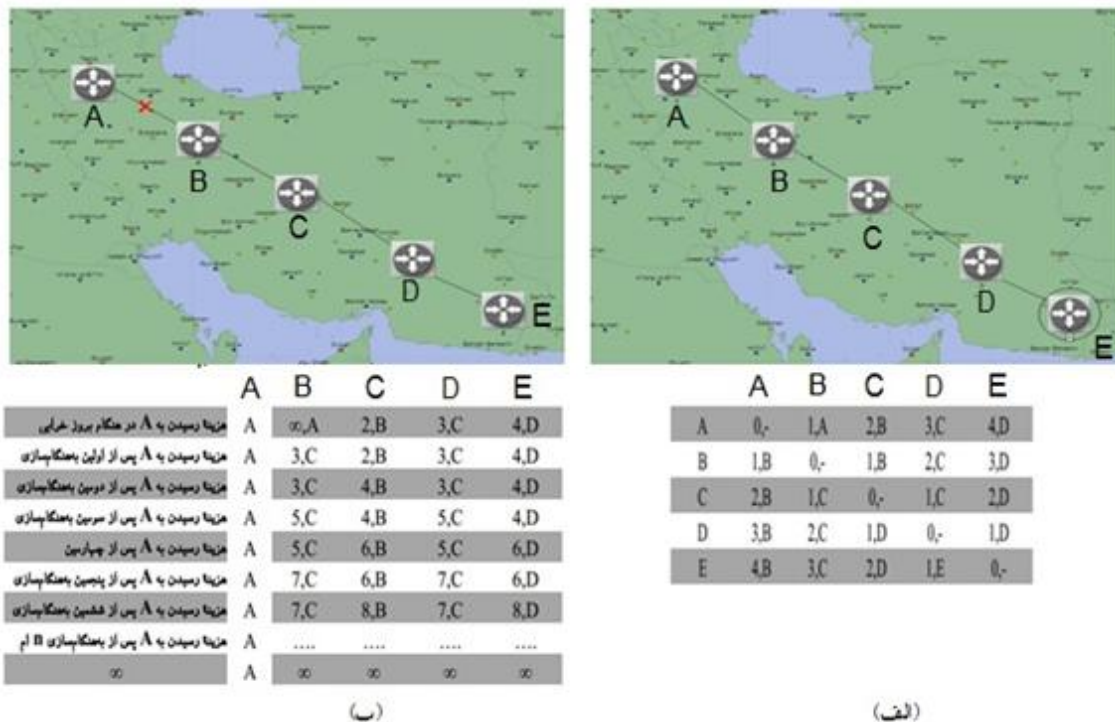
1 -Distance Vector Routing

2 - Routing Information Protocol

### ۳-۷ مسئله بی نهایت گرایی

مسیریابی بردار فاصله از نظر تئوری کار می کند، اما در عمل مشکل جدی دارد با این که پاسخ صحیح می دهد، ولی به کندی به خبرهای خوب عمل می کند، ولی به خبرهای بد واکنش سریع نشان می دهد. برای مشاهده چگونگی انتشار خبرهای خوب، زیر شبکه پنج گره ای فرضی خطی شکل ۳-۳ را در نظر بگیرید، که در آن تعداد جهش ها به عنوان مقیاس است و هر مسیریاب فقط از طریق یک مسیر به صورت خطی به دیگری وصل می باشد. در شکل ۳-۳ الف به طور فرضی زیر شبکه و جداول مسیریابی آن را مشاهده می نمایید. البته این جدول در شرایط عادی بدست آمده است. حال در شکل ۳-۳ ب فرض کنید خط ارتباطی A تا B به هر دلیلی قطع شد. در این هنگام، همان طور که در جدول شکل ۳-۳ ب می بینید، هزینه مسیریاب از B تا A بی نهایت می شود و جدول مسیریاب ها به مرور طبق شکل تغییر خواهند کرد. چون مسیریاب ها مرحله به مرحله جداول خود را برای یکدیگر می فرستند، در مرحله اول هزینه B تا A به دلیل قطعی ارتباط بی نهایت شد. در مرحله بعد (مثلا به مدت t ثانیه) این خبر به C می رسد. C به B می گوید که من با ۲ گام به A وصل هستم. با توجه به این که B نمی داند که او از طریق خودش به A وصل بوده و این طور فرض می کند که حتما مسیر دیگری به A دارد، به این خبر خوب سریع واکنش نشان داده و خودش تا C یک گام و از C تا A هم دو گام، بنابراین در جدول خود هزینه رسیدن به A را ۳ از طریق C قرار می دهد. در این مرحله هنوز خبر به بقیه نرسیده است. در مرحله بعد B به C می گوید که من با ۳ گام به A وصل هستم. C به این خبر جدید واکنش نشان داده و با احتساب هزینه خودش تا B یعنی ۱ گام + ۳ گامی که B تا A اعلام کرده، در جدول خود هزینه رسیدن به A را ۴ از طریق B قرار می دهد. در مرحله بعد این خبر های جدید به مسیریاب D هم می رسد. مسیریاب C به B می گوید که من با ۴ گام به A وصل هستم. مسیریاب B هم به این خبر جدید واکنش نشان داده و با احتساب هزینه خودش تا C یعنی ۱ گام (۱+۴)، در جدول خود هزینه رسیدن تا A را ۵ از طریق C قرار می دهد. به همین ترتیب C به D می گوید که من با ۴ گام از طریق B به A وصل هستم. مسیریاب D نیز به این خبر جدید واکنش نشان داده و با احتساب هزینه خودش تا مسیریاب C (۱+۴)، در جدول خود هزینه رسیدن به A را ۵ از طریق C قرار می دهد. در مرحله بعد این خبر نیز به مسیریاب E نیز می رسد. در این مرحله B به C می گوید که با ۵ گام به A وصل می باشد. البته مسیریاب D نیز به C همین فاصله ۵ گام را می دهد. مسیریاب C نیز به این خبر جدید واکنش نشان داده و با انتخاب یکی از آن ها یعنی مسیریاب B، طبق روال قبل، جدول خود را با هزینه ۶ گام برای رسیدن به A بروز رسانی می کند. مسیریاب D نیز به E همین فاصله را می گوید و مسیریاب E هم با توجه به این

خبر جدید و با احتساب هزینه خودش تا D یعنی ۱ گام (۵+۱)، در جدول خود فاصله تا A را ۶ از طریق D قرار می دهد. و همان طور که در شکل می بینید، به همین ترتیب این روند افزایشی ادامه پیدا می کند.



شکل ۳-۳ (شمارش تا بی نهایت) - عدم همگرایی سریع

با توجه به مثال بالا، واکنش این الگوریتم به خبرهای خوب و بد را دیدیم. گاهی تمام مسیر یاب ها بی نهایت بار کار می کنند. به همین دلیل، عاقلانه است که بی نهایت را برابر با طولانی ترین مسیر به علاوه ۱ قرار داد. اگر مقیاس تاخیر زمان باشد هیچ حد بالایی تعریف شده ای وجود ندارد، مگر آن که حد بالا را آنقدر زیاد فرض کنیم که با مسیری که به طور طبیعی تاخیر آن بالا است به عنوان مسیر از کار افتاده و خراب رفتار نشود. این مسئله بی نهایت گرایی نام دارد. تلاش زیادی برای حل آن انجام شد، ولی هیچ کدام موفق نبوده اند. مسئله مهم این است که وقتی A به B می گوید مسیری در اختیار دارد، B نمی تواند بفهمد که آیا خودش در آن مسیر قرار دارد یا خیر.

### ۸-۳ الگوریتم حالت لینک (پیوند)<sup>۱</sup>

مسیریابی بردار فاصله مسیریابی خوبی بود و حتی در شبکه آرپانت ۱۰ تا سال ۱۹۷۹ نیز عملیاتی بود، اما دو مشکل اساسی داشت. نخست اینکه معیار تاخیر در این الگوریتم، طول صفی از مسیر یاب ها بود و دوم اینکه پهنای باند هر یک از خطوط در محاسبات دخالت داده نمی شد. بنابراین حتی اگر جای فاصله را با پهنای باند در جداول

مسیریاب عوض می کردند، زمان همگرایی این مسیریاب ها به یک نتیجه درست، به بی نهایت میل می کرد . الگوریتم حالت لینک ، ساده است و می توان به صورت زیر آن را بیان کرد:

(۱) همسایه هایش را تشخیص داده و آدرس شبکه آنها را بداند.

(۲) تاخیر یا هزینه تا همسایه هایش را اندازه گیری کند.

(۳) ایجاد بسته ای که اطلاعات به دست آمده از همسایه ها را نگهداری کند.

(۴) این بسته ها را به تمام مسیریاب ها ارسال نماید.

(۵) کوتاهترین مسیر به هر مسیر دیگر را محاسبه کند.

با این روش کل توپولوژی و تمام تاخیرها به طور آزمایشی اندازه گیری می شود و به مسیر یاب های دیگر توزیع می گردد. سپس الگوریتم دایجکسترا می تواند برای یافتن کوتاهترین مسیر به مسیر یاب های دیگر مورد استفاده قرار گیرد . شناسایی همسایه ها به این صورت انجام می گیرد که پس از راه اندازی مسیریاب (بوت شدن) یک بسته سلام به تمام همسایه ها ارسال می شود. مسیریاب های همسایه مشخصات خود را برای این مسیریاب می فرستند . برای تخمین هزینه و تاخیر همسایه ها، از بسته ای به نام Echo استفاده می شود. وقتی مسیریاب این بسته را برای همسایه می فرستد، آن مسیریاب فوراً باید پاسخ آن را ارسال کند، پس از محاسبه زمان رفت و برگشت و تقسیم آن بر عدد ۲، میزان نسبی تاخیر بدست می آید. حتی برای نتایج بهتر، این کار را می توان چند بار انجام داد و میانگین را مورد استفاده قرار داد. در این روش به طور ضمنی فرض می شود که تاخیرها متقارن اند. درحالی که همیشه این طور نیست. موضوع جالب این است که آیا هنگام اندازه گیری تاخیر، بار را باید در نظر گرفت یا خیر ؟ برای در نظر گرفتن بار، تایمر رفت و برگشت باید از زمانی که Echo در صف قرار می گیرد. شروع به کار کند برای صرف نظر از بار، تایمر رفت و برگشت باید از زمانی که Echo به جلوی صف رسیده باشد را در نظر گرفت . سپس این اطلاعات را در قالب بسته ای برای دیگر مسیریاب ها ارسال می کند تا آنها نیز از وضعیت این مسیریاب مطلع باشند. وقتی اطلاعات مورد نیاز برای مبادله جمع آوری شد قدم بعدی هر مسیریاب این است که بسته ای حاوی تمام داده ها ایجاد کند. در ابتدای هر بسته ، هویت فرستنده قرار می گیرد، سپس شماره ترتیب و سن قرار دارد و تعدادی از همسایه ها به دنبال آن قرار می گیرند . ساخت بسته های حالت پیوند ساده است. بخش مشکل آن تعیین زمان ساخت آنها است . یک راه حل این است که به طور دوره ای ساخته شوند. یعنی، در فواصل زمانی ایجاد گردند. روش دیگر این است که وقتی رویدادهای مهمی مثل از کار افتادن خط یا همسایه و فعال شدن دوباره آنها یا تغییر خواص آن، اتفاق می افتد ایجاد گردد. مبحث دیگر بخش الگوریتم ، توزیع قابل اعتماد بسته های حالت پیوند است. وقتی بسته ها توزیع شدند و در خط قرار گرفتند . اولین مسیر یاب که اولین بسته



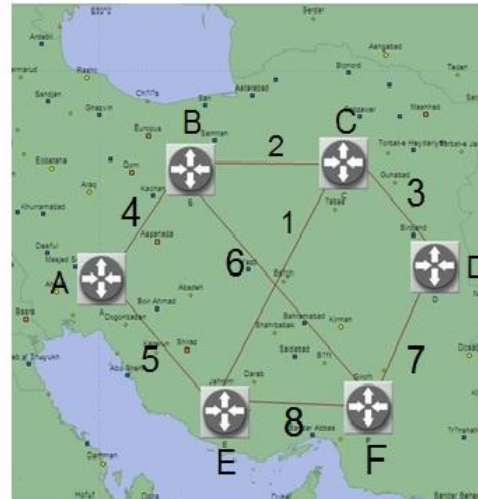
ها را دریافت می کند ، مسیرهای خود را تغییر می دهد . در حالی که ممکن است بقیه هنوز چنین کاری نکرده باشند. در نتیجه مسیریاب های مختلف ممکن است برای لحظاتی نسخه هایی گوناگونی از توپولوژی زیر شبکه را به کار گیرند ، و این کار منجر به مشکلاتی در مسیریابی صحیح ، بروز حلقه بینهایت ، ماشین های غیر قابل دستیابی و سایر مشکلات شوند. ابتدا، الگوریتم توزیع اولیه را مورد بحث قرار می دهیم. سپس اصلاحاتی را بر روی آن انجام می دهیم. ایده اصلی ، استفاده از الگوریتم غرق کردن برای توزیع بسته های حالت پیوند است برای کنترل غرق کردن ، هر بسته حاوی شماره ترتیبی است که با ارسال هر بسته ، یک واحد افزایش می یابد. وقتی بسته حالت پیوند دیگری دریافت می شود ، با لیستی از بسته ها که تاکنون دیده شده اند مقایسه می شود . هرگاه بسته ای دریافت شود. به هر خطی به جز خطی که از آن آمده است، توزیع می گردد. و اگر تکراری باشد، صرف نظر می شود اگر بسته ای دریافت شود که شماره ترتیب آن کوچک تر از بالاترین شماره ای باشد که تاکنون مشاهده شده است به دلیل کهنه بودن رد می شود . این الگوریتم دارای مشکلات خاصی است اما این مشکلات قابل کنترل اند. یکی این که اگر شماره ها تمام شدند، بسته های بعدی از اول شماره گذاری شوند. راه حل این مشکل، استفاده از شماره ترتیب ۳۲ بیتی است . دوم اینکه اگر مسیریاب از کار افتد ، شماره ترتیب خود را از دست می دهد. اگر مجدداً از صفر شروع کند، بسته بعدی به عنوان بسته تکراری رد خواهد شد. سوم اینکه اگر شماره ترتیب خراب شود مثلاً ۶۵۵۴۰ به جای ۴ (خطای یک بیتی ) دریافت شود ، بسته های ۵ تا ۶۵۵۴۰ به علت کهنگی رد می شوند زیرا فرض می شود که شماره ترتیب باید ۶۵۵۴۰ باشد. راه حل این مشکلات این است که طول عمر هر بسته بعد از شماره ترتیب قرار داده شود و هر ثانیه یک واحد از آن کسر گردد . وقتی که طول عمر به صفر رسید. از اطلاعات حاصل از آن مسیریاب صرف نظر می شود.

اصلاحاتی در این الگوریتم توانمندی آن را زیاد می کند. وقتی بسته حالت پیوند به مسیریاب می آید تا ارسال شود فوراً برای انتقال در صف قرار نمی گیرد. بلکه به ناحیه نگهدارنده ای می رود تا مدت کوتاهی را منتظر بماند. اگر قبل از انتقال آن ، بسته دیگری از همان منبع برسد، شماره ترتیب آنها مقایسه می شود اگر باهم برابر باشند بسته تکراری نادیده گرفته می شود، اگر مساوی نباشند ، قدیمی تر، نادیده گرفته می شود. برای حفاظت در مقابل خطاها ، در مسیریاب تمام بسته های حالت پیوند اعلام وصول می شوند وقتی خط آزاد می شود ناحیه نگهدارنده به طریق نوبتی پیمایش می شود. تا بسته یا اعلام وصولی را برای ارسال انتخاب نماید. وقتی مسیریاب مجموعه کاملی از بسته های حالت پیوند را جمع آوری کرد ، می تواند گراف کامل زیر شبکه را ایجاد نماید و الگوریتم دایجکسترا را می توان اجرا کرد تا کوتاه ترین مسیر به همه مقصد ها را بیابد . نتایج این الگوریتم می تواند در

جدول مسیریابی قرار گیرد. مسیریابی حالت پیوند در شبکه های واقعی به طور گسترده به کار رفته است. مانند پروتکل های مسیریابی  $IS-IS^2$ ،  $OSPF^1$

نام مسیریاب	A	B	C	D	E	F
شماره ترتیب	Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
طول عمر	Age	Age	Age	Age	Age	Age
	B 4 E 5	A 4 C 2 F 6	B 2 D 3 E 1	C 3 F 7	A 5 C 1 F 8	B 6 D 7 E 8

(ب)



(الف)

شکل ۳-۴ (الف) یک زیر شبکه (ب) بسته های حالت لینک (LS) برای این زیر شبکه

### ۳-۹ مسیریابی سلسله مراتبی<sup>۳</sup>

با بزرگ شدن اندازه شبکه، جدول های مسیریابی مسیریاب نیز به تناسب آن رشد می کنند. با بزرگ شدن اندازه جدول ها، نه تنها حافظه مصرف شده بیشتر می گردد، بلکه زمان لازم برای جست و جو در جدول بیشتر می شود. و برای گزارش وضعیت آنها به پنهان باند بیشتری نیاز است. ممکن است شبکه ها به حدی رشد کنند که دیگر امکان نداشته باشد که هر مسیریاب برای هر مسیریاب دیگر دارای یک درایه باشد، لذا مسیریابی به صورت سلسله مراتبی انجام می شود. مانند شبکه تلفن. وقتی مسیریابی سلسله مراتبی به کار گرفته می شود، مسیریاب ها به ناحیه هایی تقسیم می شوند به طوری که هر مسیریاب در ناحیه خودش تمام جزئیات مربوط به چگونگی ارسال بسته ها به مقصدها را می داند اما از ساختار داخلی سایر ناحیه خبر ندارد. وقتی شبکه های مختلفی به هم وصل می شوند. طبیعی است که باید به صورت ناحیه های جداگانه در نظر گرفته شوند تا نیاز نباشد مسیریاب های موجود در یک شبکه، از ساختار توپولوژی مسیریاب های دیگر اطلاع داشته باشند.

### ۳-۱۰ مسیریابی فراگیر<sup>۴</sup>

- 1 - Open Shortest Path First
- 2 - Intermediate System to Intermediate System
- 3- Hierarchical Routing
- 4- Broadcast Routing

در بعضی از کاربردها میزبانها می خواهند پیام هایی را به تمام یا بعضی از میزبانها ارسال کنند، بعنوان مثال خدمات توزیع گزارشات هواشناسی، بازسازی های بازار سهام، یا برنامه رادیویی روزمره، ارسال همزمان بسته ای به تمام مقصدها، اصطلاحاً پخش فراگیر نام دارد. برای انجام آن راههای گوناگونی پیشنهاد نموده اند. روش اول که نیاز به ویژگی خاصی از زیر شبکه ندارد، این است که منبع، بسته متفاوتی را به تمام مقصدها بفرستد. روش دوم، استفاده از روش غرق کردن یا سیل آسا است. روش سوم استفاده از الگوریتم مسیریابی مقصدهای چندگانه (چند مقصدی) است. چهارمین روش، استفاده از یک درخت پوشای مناسب است. روش دیگر الگوریتم پخش فراگیر، این است که حتی هنگامی که مسیر یاب اطلاعاتی راجع به درختهای پوشا نداشته باشد، سعی می کند رفتار الگوریتم درخت پوشا را تخمین بزند. این ایده، پیشروی مسیر معکوس نام دارد.

### ۱۱-۳ مسیریابی چند پخش<sup>۱</sup>

در بعضی از کاربردها فرایندهای مستقل از هم به صورت گروهی کار می کنند، مانند گروهی از فرایندها که سیستم بانک اطلاعاتی توزیعی را پیاده سازی می کنند. در اغلب موارد لازم است یکی از فرایندها پیامی را به سایر اعضای گروه ارسال نماید. اگر گروه کوچک باشد، می تواند پیام نقطه به نقطه را به تمام اعضا صادر کند. اگر گروه بزرگ باشد، این راهبرد گران تمام می شود. گاهی می توان از پخش فراگیر استفاده کرد، اما استفاده از پخش فراگیر برای اطلاع دادن به ۱۰۰۰۰ ماشین در شبکه ای با میلیونها گره کارآمد نیست، زیرا اغلب گیرنده ها علاقه ای به پیام ندارند (حتی در حالت بدتر، علاقه دارند ولی اجازه دیدن آن را ندارند). بنابراین باید بتوانیم پیام را به گروهی بفرستیم که اندازه آن گروه از نظر عددی بزرگ باشد ولی در مقایسه با کل شبکه کوچک باشد. ارسال پیام به چنین گروهی چند پخش نام دارد و الگوریتم مسیریابی آن، مسیریابی چند پخش نامیده می شود.

### ۱۲-۳ مسیریابی برای میزبان های سیار

امروزه با پیشرفت تکنولوژی، میلیونها نفر کامپیوترهای سیار دارند و علاقه مند هستند در هر جا به اینترنت دسترسی داشته و فایل اطلاعات خود را مشاهده و ویرایش نمایند. این میزبان های سیار<sup>۲</sup> موجب پیچیدگی جدیدی در شبکه می شوند. در هدایت بسته ای به میزبان سیار، شبکه باید ابتدا آن را بیابد. موضوع ملحق شدن میزبان های سیار به شبکه موضوعی است که با مشکلاتی همراه می باشد. در اینجا این نوع مسیریابی را بررسی خواهیم نمود.



شکل ۳-۵ یک شبکه WAN که شبکه های LAN، MAN و سلولهای بی سیم بدان متصل شده اند

مدل میانی که طراحان از آن استفاده می کنند در شکل ۳-۵ آمده است در اینجا یک شبکه گسترده وجود دارد که حاوی مسیر یابها و میزبانها می باشد. شبکه های محلی و شهری و سلول های بی سیم به این شبکه گسترده متصل اند. میزبان هایی که حرکت نمی کنند (ثابت اند) از طریق سیم های مسی یا فیبر نوری به شبکه وصل می شوند. بر عکس دو نوع میزبان دیگر وجود دارند. میزبانهای مهاجر میزبانهای ثابتی اند که گاهی از یک سایت ثابت به سایت ثابت دیگر منتقل می شوند اما فقط وقتی از شبکه استفاده می کنند که به طور فیزیکی به آن وصل باشند. میزبانهای متحرک کسانی هستند که در حال حرکت نیز به شبکه متصل اند. این دو نوع میزبان را میزبانهای سیار می نامند. فرض می شود تمام میزبانها موقعیت داخلی ثابتی داشته باشند که هرگز تغییر نکند. میزبانها آدرس داخلی ثابتی نیز دارند که محل آنها را مشخص می کند. هدف مسیریابی در سیستمی با میزبانهای سیار، عبارت است از: ارسال بسته ها به میزبانهای سیار به کمک آدرسهای داخلی آنها، و خواندن بسته ها توسط میزبانها در هر جایی که هستند. در مدلی، جهان (از نظر جغرافیایی) به واحدهای کوچکی تقسیم شده است. این واحدها را ناحیه می نامیم به طوری که هر ناحیه یک شبکه محلی یا سلول بی سیم است هر ناحیه دارای یک یا چند عامل خارجی است که فرایندهایی هستند که اطلاعات تمام میزبانهای سیار ناحیه را نگهداری می کند بعلاوه هر ناحیه دارای عامل خانگی است. این عامل، اطلاعات میزبانهایی را که خانه شان در این ناحیه قرار دارد ولی فعلا با ناحیه دیگری در حال ملاقات اند نگهداری می کند.

- وقتی میزبان جدیدی وارد ناحیه ای شود، چه از طریق اتصال به آن (مثل وصل شدن به شبکه محلی)، یا سرگردان بودن در سلول، کامپیوتر باید خودش را در عامل خارجی ثبت نماید. روند ثبت به صورت زیر انجام می شود:
- (۱) هر عامل خارجی به صورت دوره ای بسته ای را پخش می کند تا وجود و آدرس خود را اعلام کند. میزبان سیار تازه وارد، ممکن است منتظر یکی از این پیامها باشد اما اگر در مدت معینی چنین پیامی نرسد، میزبان سیار می تواند بسته ای را پخش کند و بگوید آیا عامل خارجی وجود دارد؟
  - (۲) میزبان سیار، در عامل خارجی ثبت می شود. برای این کار آدرس داخلی خود (محل استقرار دائم خود)، آدرس لایه پیونده داده فعلی، و اطلاعات سری دیگر را ارائه می کند.
  - (۳) عامل خارجی با عامل خانگی میزبان سیار تماس برقرار می کند و می گوید یکی از میزبانهای شما در این جاست، پیام عامل خارجی به عامل خانگی، حاوی آدرس شبکه عامل خارجی است. همچنین حاوی اطلاعات سری است تا عامل خانگی را متقاعد کند که میزبان سیار واقعا وجود دارد.
  - (۴) عامل خانگی اطلاعات سری را که حاوی مهر زمان است، بررسی می کند تا ثابت شود در چند ثانیه قبل تولید شده است. اگر اطلاعات را تصدیق نمود، به عامل خارجی می گوید که پیشروی نماید.
  - (۵) وقتی عامل خارجی اعلام وصولی را از عامل خانگی دریافت کند یک باره در جدول خود ایجاد می نماید و اطلاع می دهد که میزبان سیار ثبت شده است.
- حال ایده آل آن است که وقتی کاربری ناحیه را ترک می کند، باید اطلاع دهد تا از ثبت خارج شود، اما اغلب کاربران به طور غیر منتظره، کامپیوترهای خودشان را خاموش می کنند. وقتی بسته ای به میزبان ارسال می گردد به شبکه محلی داخلی کاربر هدایت می شود، چون به آدرس محل استقرار دائم آن دسترسی دارد، مانند آنچه که در مرحله ۱ از شکل ۳-۶ نشان داده شده است. اینجا فرستنده ای در شهر تبریز می خواهد بسته ای را به یک میزبان سیار که محل دائمی آن مشهد است و الان در بوشهر می باشد، بفرستد. بسته های ارسال شده به میزبان سیار در LAN داخلی آن یعنی در مشهد، توسط عامل خانگی متوقف می شود. سپس عامل خانگی، محل جدید (موقتی) میزبان سیار را جستجو می کند و آدرس عامل خارجی را می یابد. عامل خانگی دو کار را انجام می دهد اول اینکه بسته را در درون فیلد داده از یک بسته بیرونی دیگر جاسازی می کند و آن را به عامل خارجی می فرستد (مرحله دو در شکل ۳-۶) این راهکار را تونل سازی می نامند؛ پس از گرفتن بسته بسته بندی شده، عامل خارجی، بسته اصلی را از درون فیلد داده آن جدا می کند و آن را به میزبان سیار می فرستد. دوم اینکه عامل خانگی به فرستنده می گوید از این پس بسته ها را با قراردادن درون یک بسته دیگر (بسته هایی که صریحاً به عامل خارجی

آدرس دهی می شوند) ، مستقیما به عامل خارجی ارسال نماید . (مرحله ۳) اکنون بسته های بعدی می توانند مستقیما از طریق عامل خارجی (مرحله ۴) به میزبان هدایت شوند (با نادیده گرفتن موقعیت داخلی).



شکل ۳-۶ مسیریابی بسته ها بسوی ماشین های متحرک

با توجه به موضوعی که مطرح شد ، بحث های زیادی را در این مورد می توان مطرح کرد و روش های مختلفی برای مسیریابی در این زمینه وجود دارد . از جمله اینکه این وظایف و اختیارات چگونه بین میزبان سیار و مسیریاب تقسیم می شود . وظایف هر کدام به چه نحوی می باشد . بعضی مسیریاب ها قادر هستند بدون هیچ دخالت بیرونی آدرس میزبان سیار را به آدرس جدیدش تغییر دهند . یا آن که در بعضی روشها احتیاجی به عامل خارجی نیست و میزبان های میهمان به محض وارد شدن در شبکه ، یک آدرس موقتی که شاید منحصر به فرد هم باشد ، را دریافت می کنند . یا روشهای تغییر آدرس و ارسال بسته ها به چه نحوی می باشد یا مسائل امنیتی مثل این که چطور این میزبان ها و مسیریاب ها به یکدیگر اعتماد کرده و بسته ها را ارسال می نمایند . مثلا اگر A به B گفت از این به بعد بسته های C را برای من بفرست ، این اعتماد سازی چطور صورت می گیرد .

### ۳-۱۳ مسیریابی در شبکه های موقتی

در بحث قبلی ، با شبکه هایی روبه رو بودیم که مسیریاب ها ثابت و میزبان ها سیار بودند . حال در مورد شبکه هایی بحث خواهیم کرد که مسیریابها نیز متحرک و سیار هستند . این گونه شبکه ها را می توان در محیط های زیر مشاهده نمود .

- (۱) وسایل نقلیه نظامی در میدان جنگ و ناوگان کشتی ها در دریا.
  - (۲) شرایط اضطراری در هنگام وقوع زلزله که زیرساخت ها را خراب کرده است.
  - (۳) گردهمایی افرادی با کامپیوترهای کیفی در منطقه ای که فاقد 802.11 است.
- در همه این موارد و موارد مشابه، هر گره هم مسیریاب و هم میزبان است که معمولاً در یک ماشین قرار دارند و شبکه هایی که از این گره ها تشکیل می شوند را شبکه های موقتی<sup>۱</sup> یا (شبکه های موردی همراه) گویند. تفاوت شبکه های موقتی با شبکه های سیمی این است که تمام قوانین مربوط به توپولوژی های ثابت، همسایگان ثابت و مشخص، رابطه ثابت بین آدرس IP و مکان، و غیره باید نادیده گرفته و مسیریاب ها دائماً در حال جابجایی می باشند. در شبکه سیمی مسیرهای معتبر به مقصد، همواره معتبر خواهد بود (مگر اینکه سیستم خراب شود) ولی در شبکه های موقتی، توپولوژی ممکن است بدون هیچ اختار و هماهنگی قبلی تغییر نماید و این تغییر همواره وجود داشته باشد. با توجه به این شرایط، مسیریابی در شبکه های موقتی راهکار و ساختار منحصر به فرد خود را می طلبد. الگوریتم های مسیریابی گوناگونی مانند:
- DSDV, WRP, CGSR, FSR, ZHLS, AODV, DSR, OLSR, SDR, TORA, SAODV, HSR, ARAN و .... برای شبکه های موقتی پیشنهاد شدند.

### ۳-۱۴ جمع بندی

در این فصل با مفهوم، ویژگی ها و انواع مسیریابی در فرصت کوتاهی که بود آشنا شدیم. با رشد سریع تکنولوژی و فناوری های نوین هر روز شاهد نوآوری های جدیدی در عرصه شبکه های کامپیوتری و مخابراتی هستیم و با توجه به این که شبکه های اقتضائی متحرک به دلیل نوع عملکرد و ویژگی هایی که دارند هر روز بر استفاده آن ها با کاربردهای مختلف افزوده می شود، بنابراین کار بر روی این گونه شبکه ها از اهمیت بالائی برخوردار می باشد. با توجه به مسیریابی این گونه شبکه ها و محدودیت ها و مشکلاتی که در این زمینه موجود می باشد، مخصوصاً مبحث امنیت آن، الگوریتم ها و پروتکل ها و نظرات و پیشنهادات مختلفی در این زمینه هر روز منتشر می شود و این خود حکایت از مهم بودن صورت مسئله می باشد. در این راستا در فصل آینده در مورد مسیریابی شبکه های اقتضائی متحرک بحث خواهیم نمود و تا جایی که مجال فرصت دهد در مورد روشها و الگوریتم ها و پروتکل های متعارفی که هم اکنون در این شبکه ها مورد استفاده قرار می گیرد، صحبت خواهیم کرد.

## فصل چهارم

### مسیریابی شبکه های اقتضائی



## ۴-۱ مقدمه

یکی از مهمترین مسائلی که در هر نوع شبکه ای مطرح می شود مسیریابی و پیدا کردن مسیرهای بهینه از هر مبدا به هر مقصودی می باشد، مسیریابی در شبکه های با سیم و شبکه های بی سیم دارای زیر ساخت که نقاط دسترسی در آنها ثابت هستند خود مسئله بسیار مهم و مشکلی است و نیازمند تدابیر و راه حل های خاص می باشد، حل این مسائل در شبکه های اقتضائی متحرک که گره ها ثابت نیستند و دائم در حال تغییر مکان هستند بسیار سخت تر بوده و به تمهیدات بیشتری نیاز دارد چون که این نوع شبکه ها به هیچ وجه توپولوژی ثابتی ندارند و در هر لحظه نحوه چیدمان گره ها دچار تغییر می شود ، هر چند عوامل دیگری همچون متحرک بودن و نبود سیستم کنترلی متمرکز، چند جهشی ، اندازه ی بزرگ شبکه ، نا همگونی انواع میزبان ها و تنوع نوع و ساختار آنها و محدودیت توان باتری ها این مشکلات را دو چندان کرده است. به همین جهت مسیریابی در این شبکه ها از اهمیت بالایی برخوردار بوده و مطالعه و بررسی بیشتری را می طلبد. در چنین شبکه ای، هر گره سیار نه تنها به عنوان یک میزبان بلکه به عنوان یک مسیر یاب عمل می کند، و بسته های دیگر گره های سیار را در شبکه انتقال می دهد. در نتیجه گره های سیار در شبکه بطور پویا مسیرهایی را بین خودشان ایجاد می کنند تا شبکه را بصورت شناور ایجاد کنند. اما مشکل شبکه اقتضائی متحرک این است که تمامی گره ها اگرچه قادر به حرکت و متصل ماندن به یکدیگر بصورت پویا هستند، اما در برابر عدم موفقیت، آسیب پذیر هستند. این عدم موفقیت ممکن است بخاطر ضعیف شدن باتری یا بخاطر محدودیت گره برای شرکت در شبکه باشد که ناشی از تغییر در توپولوژی است. بنابراین مسیریابی بسته ها در چنین محیطی مشکل است.

## ۴-۲ معیارهای طبقه بندی روش ها

در حالت کلی می توان گفت که هنوز طبقه بندی کامل و استاندارد برای مسیریابی در شبکه های اقتضائی بوجود نیامده و مقالات مختلف طبقه بندی های متفاوتی را برای این نوع شبکه ذکر نموده اند. شاید یکی از دلایل اینکه طبقه بندی استاندارد برای این شبکه ها وجود ندارد اینست که هنوز مرزهای دانش در این زمینه مورد دستیابی کامل قرار نگرفته و هر روز روش های جدیدی که از تکنیک جدیدی استفاده می کنند مطرح می شود، در واقع در حال حاضر روش های مسیریابی را می توان از دیدگاه های مختلفی طبقه بندی و بررسی نمود که از این گونه می توان روش های واکنشی، فعال، ترکیبی، سلسله مراتبی، برحسب موقعیت جغرافیایی، چندپخشی و چند گروه دیگر اشاره نمود ولی این طبقه بندی ها هم خیلی صحیح نمی باشد چون مثلا روش های جغرافیایی خود ممکن است از یک مشی فعال و یا واکنشی استفاده نمایند، بنابراین ما ابتدا معیارهای دسته بندی

روش های مسیریابی در شبکه های اقتضائی را مرور میکنیم و سپس در بخش بعدی دیدگاه های دیگر و همچنین چند نمونه از پروتکل ها را شرح می دهیم . از دیدگاه های مختلفی می توان این دسته بندی های مختلف را به وجود آورد که مهمترین آنها عبارتند از :

#### ۴-۲-۱ از دیدگاه نوع ذخیره کردن اطلاعات مسیریابی

از این لحاظ پروتکل های مسیریابی را می توان به دو دسته تقسیم بندی نمود که روش مسیریابی حالت لینک و روش مسیریابی بردار مسافت نام دارند . در روش مسیریابی حالت لینک اطلاعات مسیریابی در فرم بسته های حالت لینک رد و بدل می شود، هر تغییر لینکی باعث ایجاد یک حالت لینک و ارسال سیل آسای آن به کل شبکه می شود. هر گره از روی حالت لینک های دریافتی یک توپولوژی شبکه عمومی مجازی را ترسیم کرده و نگهداری کند و همه مسیر ها را به گره های دیگر محاسبه می کند. مشکل مسیریابی حالت لینک سر بار بیش از حد آن است، زیرا در شبکه های اقتضائی توپولوژی سرعت در حال تغییر میباشد بنابراین باید بسته های حالت لینک بسیار زیادی در شبکه رد و بدل شود که سر بار بالایی را ایجاد می نماید. در مسیریابی بردار مسافت هر گره یک بردار مسافت را که شامل سه مؤلفه است برای هر مقصدی نگهداری می کند، این مؤلفه ها عبارتند از: شناسه همه مقصدهای موجود، فاصله بر حسب تعداد گام تا هر مقصد و گام بعدی به هر مقصد. هر گره به صورت پریودیک بردارهای مسافت خود را بروزرسانی می کند. مسیر کامل به یک مقصد بایک روش توزیع شده با ترکیب گام بعدی گره ها روی مسیر از مبدأ تا مقصد ایجاد می شود. مشکل مسیریابی بردار مسافت همگرایی کند و تمایل به ایجاد حلقه می باشد. بطور کلی این نوع روش ها بیشتر در شبکه های با سیم مطرح می باشند و کاربرد دارند مانند الگوریتم های مسیریابی حالت لینک OSPF و الگوریتم مسیریابی بردار مسافت RIP.

#### ۴-۲-۲ از لحاظ بروز رسانی

اطلاعات مسیریابی باید روی گره های شبکه به منظور اطلاع و آگاهی از وضعیت لینک ها و توپولوژی شبکه به روز بمانند. از این منظر پروتکل های مسیریابی شبکه اقتضائی به دو گروه طبقه بندی می شوند، یا دارای بروزرسانی دوره ای هستند و یا بروزرسانی بر مبنای رخداد دارند.

در پروتکل های دارای بروزرسانی دوره ای اطلاعات مسیریابی بصورت پریودیک در بازه های زمانی مشخصی پخش می شوند، که این کار پروتکل ها را ساده کرده و پایایی شبکه را پشتیبانی می کند و مهمتر از همه این که گره ها را برای آگاهی از توپولوژی و حالت شبکه آگاه می کند. در روش بروزرسانی بر مبنای رخداد زمانی

بروزرسانی لازم می شود که یک رخداد مانند قطع شدن یک لینک و یا پدیدار شدن یک لینک رخ دهد، یعنی تا زمانی که تغییری در وضعیت لینک ها و توپولوژی شبکه بوجود نیامده هیچ گونه بسته بروزرسانی ارسال نمی شود، البته در شبکه هایی که پویایی گره ها خیلی بالا باشد چون توپولوژی سریع تغییر پیدا می کند بسته های بروزرسانی زیادی باید ارسال شود که پهنای باند موجود را اشغال می کنند. می توان هر دو روش فوق را با هم استفاده کرد که این مکانیزم ترکیبی نامیده می شود. مثلاً در الگوریتم بردار مسافت بر مبنای شماره ترتیب مقصد هر گره بردار مسافتش را بصورت پررودیک پخش می کند و هر زمان هم که لینکی دچار تغییر شد یک پیام فوری بروزرسانی در شبکه منتشر می شود.

#### ۴-۲-۳ از لحاظ کنترل

در هر پروتکل مسیریابی باید مشخص شود که یک مسیر در کجا و چگونه محاسبه می شود. دو نوع روش کنترل برای پروتکل های مسیریابی ارائه شده است: روش کنترل متمرکز که در این روش هر گره اطلاعات کامل و عمومی از توپولوژی کل شبکه را نگهداری می کند بطوریکه گره هر وقت خواست، می تواند خودش مسیر به مقصد را محاسبه کند. مثل روشهای مسیریابی حالت لینک. روش دیگر کنترل توزیع شده که در آن هر گره فقط اطلاعات جزئی و محلی در مورد توپولوژی شبکه را نگهداری می کند و وقتی که یک مسیر باید محاسبه شود تعداد زیاد گره برای محاسبه مسیر با هم همکاری می کنند. مانند روش های بردار مسافت و مکانیزم کشف مسیر در روش های بر حسب تقاضا.

#### ۴-۲-۴ از لحاظ نوع محاسبه مسیر

اگر از این دیدگاه روش ها را بررسی نماییم دو نوع مسیریابی مرحله به مرحله و مسیریابی از مبدأ می بینیم که در مسیریابی مرحله به مرحله مسیر به یک مقصد در گام بعدی گره ها در طول مسیر توزیع می شود، وقتی گرهی یک بسته را برای یک مقصد دریافت می کند آن را به گام بعدی در امتداد مسیر می فرستد یعنی اینکه مبدأ از مسیر کامل تا مقصد اطلاعی ندارد و فقط بسته را تحویل گره بعدی می دهد و این فرایند تا رسیدن بسته به مقصد ادامه پیدا میکند، مشکل آن اینست که همه گره ها باید اطلاعات مسیریابی را نگهداری کنند و نیز اینکه ممکن است حلقه ایجاد شود. در روش های مسیریابی از مبدأ، گره مبدأ تمام گره های در طول مسیر را که باید توسط بسته پیموده شوند در هدر بسته داده قرار می دهد و گره های میانی فقط این بسته را بر اساس مسیری که در سرایند هر بسته قید شده هدایت و ارسال می کنند، یعنی هر گره میانی بسته را به گرهی تحویل میدهد که در هدر بسته مشخص شده است. در این روش گره های میانی نیازی به اطلاعات مسیریابی به روز ندارند زیرا که خود

بسته حاوی همه اطلاعات لازم می باشد، اگر این روش با روش بر حسب تقاضا همراه شود نیاز به اعلان مسیر را بصورت دوره ای از بین می برد. مهمترین نمونه از این پروتکل ها ، پروتکل مسیریابی از مبدا پویا می باشد.

#### ۴-۲-۵ از لحاظ ساختار

از دید ساختار، پروتکل های مسیریابی یا ساختار مسطح دارند و یا دارای ساختار سلسه مراتبی هستند، در ساختار مسطح همه گره ها در یک سطح از نظر اطلاعات قرار دارند، این روش برای شبکه های کوچک خوب است، در شبکه های بزرگ حجم اطلاعات مسیریابی زیاد شده و زمان زیادی برای رسیدن به یک گره دور طول می کشد. در ساختار سلسه مراتبی در شبکه های بزرگ جمعی از گره ها در شبکه بصورت پویا به قسمت هایی بنام کلاستر افزای می شوند. از تجمع کلاسترها، کلاسترهای بزرگتر ایجاد می شوند و به همین ترتیب سلسله مراتبی از کلاسترها ایجاد می شود، سازماندهی شبکه بصورت کلاستر به پلایایی توپولوژی شبکه کمک می کند. فقط اطلاعات سطح بالا و پایدار مثل سطح بالای کلاستر روی مسافت های دور منتشر می شود، بنابراین ترافیک کنترلی یا سربار مسیریابی به مقدار زیادی کاهش می یابد. داخل هر کلاستر گره ها اطلاعات کاملی از توپولوژی شبکه داخل کلاستر خودشان دارند و ممکن است مسیریابی فعال استفاده شود، اگر مقصد در کلاستر دیگری باشد مسیریابی بین کلاسترها نیاز خواهد بود که عموماً واکنشی می باشد یا ترکیبی از فعال و واکنشی است.

#### ۴-۳ پروتکل های مسیریابی متداول در شبکه های اقتضائی

پروتکل مسیریابی مکانیزمی است که به وسیله آن ترافیک کاربر از نود مبدا به مقصد فرستاده می شود. بیشینه کردن عملکرد شبکه از دیدگاه کاربرد ، همزمان با کمینه کردن هزینه شبکه مطابق ظرفیت آن ، مساله ای است که در اینجا مطرح است. مساله ای که از دیدگاه کاربرد لازم می باشند عبارتند از: تعداد پرش ها ، تاخیر ، توان ، نرخ تلف ، پایداری ، لرزش ، هزینه و ظرفیت شبکه تابعی از منابع در دسترس در هر نود و تعداد نودها در شبکه ها است . قبل از بررسی این پروتکل ها باید توجه کنیم که هدف از الگوریتم ها و استراتژی های مسیریابی جدید کاهش سربار ناشی از مسیریابی در کل شبکه ، یافتن مسیرهای کوتاه تر و انتقال صحیح داده ها و اطلاعات می باشد . چهار هسته اصلی مسیریابی برای شبکه های اقتضائی سیار عبارتند از:

(۱) ایجاد مسیر: مسیرها را مطابق اطلاعات وضعیت گردآوری شده و توزیع شده شبکه و کاربرد ایجاد می کند .

(۲) انتخاب مسیر: مسیرهای مناسب را بر مبنای اطلاعات وضعیت شبکه و کاربرد انتخاب می کند .

(۳) فوروارد کردن دیتا: ترافیک کاربرد را در مسیر انتخاب شده فوروارد می کند .

۴) نگهداری و حفاظت مسیر: نگهداری و حفاظت از مسیر انتخاب شده .

تقسیم بندی دیگری در مورد پروتکل های مسیریابی شبکه های اقتضائی وجود دارد که از این میان می توان به ۲

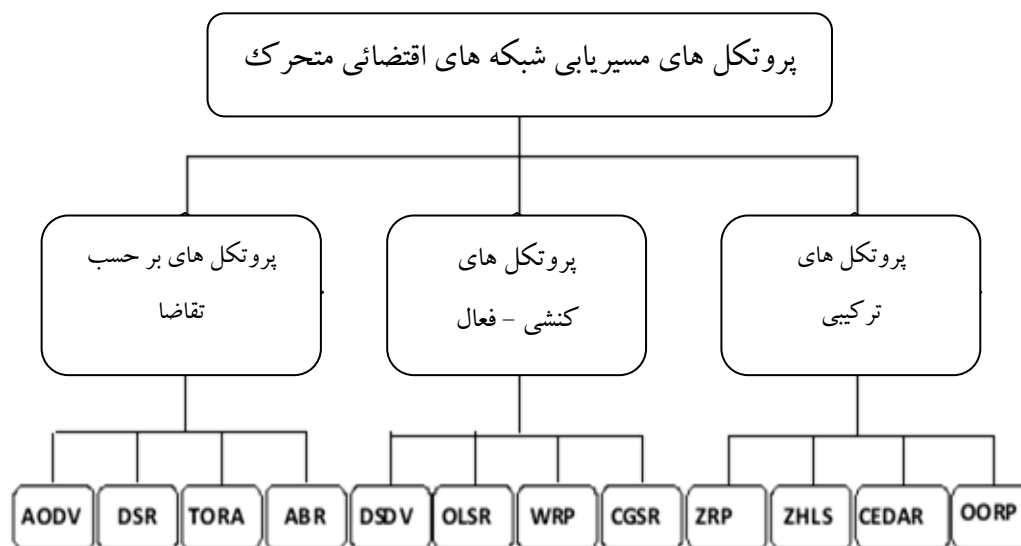
نوع زیر اشاره کرد :

تقسیم بندی اول :

پروتکل های کنش گرا - فعال ( بر حسب جدول)<sup>۱</sup>

پروتکل های واکنشی ( بر حسب تقاضا)<sup>۲</sup>

پروتکل های ترکیبی - پیوندی ( بر حسب جدول و بر حسب تقاضا)<sup>۳</sup>



شکل ۴-۱ طبقه بندی پروتکل های مسیریابی در شبکه های اقتضائی

تقسیم بندی دوم :

پروتکل های مسیریابی تخت ( مسطح)<sup>۴</sup>

پروتکل های مسیریابی سلسله مراتبی<sup>۵</sup>

پروتکل های مسیریابی بر حسب موقعیت جغرافیایی<sup>۶</sup>

#### ۴-۳-۱ پروتکل های تقسیم بندی اول

- 1 -Proactive(Table driven)
- 2 -Reactive(On demand)
- 3 -Hybrid(Table driven & On demand)
- 4 - Flat routing protocols
- 5 -Hierarchal routing protocols
- 6 -GPS Augmented geographical routing protocols

### ۴-۳-۱-۱ پروتکل های کنش گرا - فعال ( بر حسب جدول)

در پروتکل های از این نوع ، نودها مدام در حال جستجوی اطلاعات مسیریابی جدید درون شبکه هستند به صورتی که حتی با تغییر مکان نود ها در صورت نیاز به راحتی می توان مسیر مناسبی را یافته و برای ارسال و دریافت اطلاعات بین هر دو نودی استفاده کرد . به عبارت بهتر می توان گفت که در این شبکه ها مسیر ها از قبل موجود هستند. و به محض آنکه نودی اقدام به ارسال داده به نود دیگری کند قادر خواهد بود مسیر موجود را از روی اطلاعات از قبل جمع آوری شده شناسایی کرده و مورد استفاده قرار دهد و لذا تاخیری در این مورد متوجه نود نیست. در پروتکل های مسیریابی بر حسب جدول ترینال ها و مسیریاب ها یک جدول مسیریابی از همه شبکه می سازند از این رو این دسته پروتکل ها شباهت زیادی با پروتکل های مسیریابی شبکه های ثابت دارند .

پروتکل های مسیریابی بر حسب جدول اطلاعات مسیریابی برای داده ها از هر گره به گره دیگر در شبکه هماهنگ می کنند. این پروتکل ها نیاز دارند که هر گره از یک یا چند جدول برای نگهداری اطلاعات مسیریابی استفاده کند. و این جدولها با استفاده از به روز کردن خودشان به تغییرات در توپولوژی (جغرافیایی) شبکه پاسخ می دهند. مناطقی که از لحاظ جغرافیایی متفاوت هستند به تعدادی جدول های مخصوص جغرافیایی شبکه و روشهای تغییر در ساختمان شبکه نیاز دارند. در بخش زیر بعضی از پروتکل های مسیریابی بر حسب جدول مورد بحث قرار می گیرد :

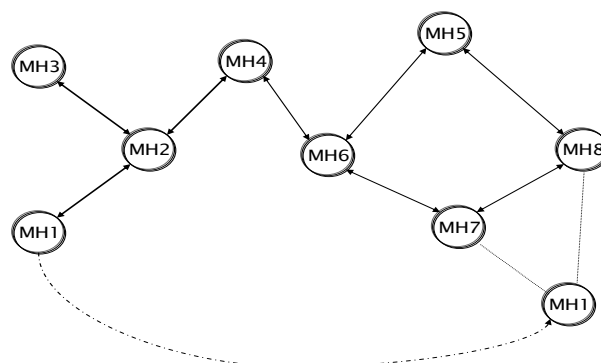
#### ۴-۳-۱-۱-۱ پروتکل مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد DSDV<sup>۱</sup>

الگوریتم مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد یک پروتکل مسیریابی گام به گام است که از مکانیزم مسیریابی بلمن فورد توسعه یافته استفاده می کند. در این روش هر گره بروزرسانی های مسیر را پخش می کند و در آن آزادی حلقه ها تضمین می شود. هر گره یک جدول مسیریابی را نگهداری می کند که شامل همه مقصدها، تعداد گام ها تا رسیدن به هر مقصد و شماره ترتیب منطبق با گره مقصد می باشد. این شماره ترتیب برای مشخص کردن مسیر های قدیمی استفاده می شود، در واقع هر مسیری که شماره ترتیب مقصد آن بزرگتر باشد مسیر جدیدتری است و این برای اجتناب از ایجاد حلقه استفاده می شود، به اینصورت که همیشه مسیرهایی استفاده می شود که شماره ترتیب بزرگتری دارد یعنی جدیدتر هستند. دلیل اینکه استفاده از مسیر های قدیمی ممکن است باعث ایجاد حلقه شود اینست که چون گره ها در شبکه اقتضائی همواره در حال تغییر مکان هستند یک گره ممکن طوری تغییر مکان دهد که در مسیر دارای حلقه قرار بگیرد. بازیابی های مسیر روی کل شبکه

1 -Destination Sequenced Distance Vector

ارسال می شود، این بازیابی ها بصورت دوره ای هر بار بعد از یک بازه زمانی خاص و نیز هر زمان که تغییری در یکی از لینک های شبکه و یا توپولوژی شبکه اتفاق بیفتد انجام می گیرد، یعنی هم بر حسب زمان هستند و هم بر حسب رخداد. این ارسال بازیابی ها با افزایش مقدار شماره ترتیب همراه است یعنی هر گرهی که یک بازیابی را به کل شبکه ارسال می کند مقدار شماره ترتیب تمامی مسیرهای جدیدی را که اعلان می کند با مقدار ثابتی افزایش می دهد. و گره هایی که این بازیابی ها را دریافت می کنند بردار مسافت خود را بروز رسانی می کنند. در ضمن هر گره در جدول مسیر یابیش گره بعدی را برای مقصدهای مختلف نگهداری می کند تا بداند که هر گره مقصد از چه طریقی قابل دسترس است. از آنجائی که بازیابی ها باید روی کل شبکه ارسال شود امکان ایجاد ترافیک بالایی روی شبکه وجود دارد، برای کاهش دادن این ترافیک بازیابی ها دو نوع بسته را بنام بسته های نسخه برداری کامل و توسعه ای بکار می برند. در بسته های نسخه برداری کامل، بسته همه اطلاعات ممکن مسیریابی را حمل می کند، یعنی این نوع بسته ها سائز بزرگی دارند ولی بسته های توسعه ای تغییرات نسبت به آخرین باری که بسته بازیابی نسخه برداری کامل ارسال شده فرستاده می شود. از بسته های نسخه برداری کامل بندرت استفاده می شود چون که شبکه آنقدر در یک لحظه تغییر نمی کند که نیاز به این نوع بسته باشد، مگر در شبکه هایی که پویایی در آنها بسیار بالا باشد. در شبکه های اقتضائی با پویایی معمولی بیشتر از بسته های توسعه ای استفاده می شود و این بسته ها معمولا در اندازه استاندارد NPDU ارسال می شوند. وقتی گره چند مسیر را به یک مقصد دریافت می کند مسیری را انتخاب می کند که شماره ترتیب بزرگتری دارد، اگر دو مسیر شماره ترتیبشان یکسان بود مسیری انتخاب می شود که پارامتر کوچکتری داشته باشد، این پارامتر می تواند تعداد گره های روی مسیر تا آن مقصد باشد. وقتی که یک گره مثل A مسیرش به گره همسایه ای مثل B شکسته شود، مسیر به B را با یک پارامتر نامتناهی و یک شماره ترتیب که از شماره ترتیب قبلی بزرگتر است را به کل شبکه اعلان می کند. از آنجایی که این شماره ترتیب به مقصد B بزرگترین شماره ترتیب است و با توجه به اینکه دارای پارامتر بینهایت است گره B برای سایر گره ها غیر قابل دسترس می باشد تا زمانی که یک شماره ترتیب بزرگتر در بازیابی های بعدی اعلان شود. هر گره همچنین زمان مقیم شدن مسیر ها را نگهداری می کند، گره ها می توانند با به تاخیر انداختن ارسال بازیابی های مسیر ها به اندازه زمان مقیم شدن ترافیک را کاهش داده و مسیر ها را با از بین بردن ارسال هایی که قرار است اتفاق بیفتد در حالیکه مدت زمان خیلی کمی از کشف مسیر بهتر جدید گذشته است بهینه کنند. در شکل ۴-۲ یک مثال از بازیابی در این پروتکل نشان داده شده است. در این شکل گره MH1 ابتدا در مجاورت گره MH2 قرار دارد، پس از مدت زمان کوتاهی بعثت پویایی شبکه این گره تغییر مکان داده و در مجاورت گره های MH7, MH8 قرار می گیرد و اتصالش با گره MH2 بطور مستقیم قطع می گردد. در

شکل جدول مسیریابی گره MH4 برای هر دو حالت قبل و بعد از حرکت نشان داده شده است. همانطور که در شکل مشاهده می شود گره MH4 به هریک از گره های دیگر مسیری دارد که با یک شماره ترتیب مشخص شده است و پارامتری هم برای هر مقصد در نظر گرفته شده است. پس از اینکه گره MH1 تغییر مکان داده و از مجاورت MH2 دور شده و به مجاورت MH7, MH8 در می آید مسیرها دیگر مسیرهای سابق نیستند و بدرد نمی خورند، بنابراین گره جدول مسیریابی را باز یابی کرده و برای اینکه مسیرهای جدید از مسیرهای قدیمی قابل تشخیص باشند مقدار شماره ترتیب را نسبت به هر مقصد به اندازه ۱۱۰ واحد افزایش می دهد، مثلاً مسیرش به گره MH8 قبل از تغییر مکان دارای شماره ترتیب 50 بوده و پس از تغییر مکان می دهد مسیر جدیدش به این گره دارای شماره ترتیب 160 می باشد و به این ترتیب کلیه باز یابی های دیگر هم انجام می شود.



Destination	Metric	Seq Number
MH1	2	S 406-MH1
MH2	1	S 128-MH2
MH3	2	S 564-MH3
MH4	0	S 710-MH4
MH5	2	S 392-MH5
MH6	1	S 076-MH6
MH7	2	S 128-MH7
MH8	3	S 050-MH8

جدول مسیریابی اعلان شده توسط گره MH4

Destination	Metric	Seq Number
MH4	0	S 820-MH4
MH1	3	S 516-MH1
MH2	1	S 238-MH2
MH3	2	S 674-MH3
MH5	2	S 502-MH5
MH6	1	S 186-MH6
MH7	2	S 238-MH7
MH8	3	S 160-MH8

جدول مسیریابی بروز شده توسط گره MH4

شکل ۴-۲ جدول مسیریابی یک گره در روش DSDV در دو زمان متوالی

معایب: این پروتکل نیازمند پارامترهایی از قبیل بازه ی زمانی به روز رسانی اطلاعات و تعداد به روز رسانی های مورد نیاز می باشد .

#### ۴-۱-۱-۳-۲ پروتکل مسیریابی بی سیم WRP<sup>۱</sup>

این پروتکل بر اساس جدول ها با هدف هماهنگ ساختن همه ی اطلاعات مسیریابی میان همه ی گره های شبکه تعریف شده است. هر گره در شبکه مسئول هماهنگ ساختن چهار جدول است:



۱- جدول مسافت ۲- جدول مسیریابی ۳- جدول هزینه پیوندها ۴- جدول لیست ارسال مجدد پیغام ها (MRL)

هر مدخل (راهرو) از MRL ، شامل تعدادی ارقام مرتب است که پیامها را به روز می کند. یک کنتور ارسال مجدد، یک پرچم که وظیفه اش تصدیق ارسال مجدد پیغامهاست، با یک مدخل در همسایگی در به روز کردن جدولها استفاده می شود. MRL پیغامهای به روز شده را با استفاده از ارسال مجدد ثبت می کند. موبایل هر یک از تغییرات لینکها را با استفاده از به روز کردن پیغامها متوجه می شوند. اگر یک گره بخواهد به شبکه اضافه شود باید یک پیام سلام صادر کند تا از متصل شدن گره به شبکه مطمئن شویم و گرنه نبود یک پیغام از یک گره به منزله شکست اتصال است. در این پروتکل گروههای مسیریابی اولاً با مقصد و ثانیاً با اطلاعات آخرین گام برای هر مقصد در شبکه های بی سیم مکاتبه می کنند. این پروتکل به کلاسی از الگوریتم های کشف مسیر با یک استثناء مهم تعلق دارد. این پروتکل بر مبنای الگوریتم کشف مسیر بنا شده با این استثنا که مشکل بی نهایت گرانی این الگوریتم را برطرف کرده است. تغییرات ایجاد شده در لینک ها از طریق ارسال و دریافت پیام میان نود های همسایه اطلاع داده می شوند .

#### ۴-۱-۳-۱-۳ پروتکل مسیریابی تغییر وضعیت دروازه سرگروه (سردسته درگاه) CGSR<sup>۱</sup>

این پروتکل در نوع آدرس دهی و به کاربردن طرحهای سازماندهی از پروتکل مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد متمایز است. در عوض از یک شبکه ی وسیع و پهن CGSR (یک دسته از شبکه های بی سیم سیار مولتی هاپ با چندین طرح مسیریابی غیر مستدل) استفاده می کند. اشخاص (کسانی که تهیه کننده ی دستورالعمل برای سیستم های CIM یا آموزش توسط کامپیوتر هستند) توضیح می دهند که چگونه با داشتن یک دسته ی کنترل سرگروهی یک گروه از گروه های شبکه اقتضائی ، یک چارچوب از کدهای مجزا ، دستیابی کانالها و تخصیص پهنای باند وسیع می توان این کار را به انجام رسانید. سرگروهها از یک الگوریتم انتخابی برای انتخاب یک گره مثل سرگروه (ریشه) استفاده می کند . این پروتکل از پروتکل مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد به عنوان طرح مسیریابی کلاستر اصلی برای نزدیکتر شدن مقصد ، اصلاح می شود. گروه های مدخل گروه هایی هستند که واسطه ارتباطی بین دو یا بیشتر کلاستر اصلی باشند. یک پکت (پیغام) وقتی که بوسیله یک گره فرستاده می شود ابتدا بر روی کلاستر اصلی قرار می گیرد، سپس پکت با استفاده از مدخلی (دروازه ای) به کلاستر اصلی دیگری فرستاده می شود تا اینکه پیغام به مقصد برسد. در این روش باید هر گره

یک جدول عضو کلاستر را در یک م کلف مخصوص برای کلاستر اصلی ذخیره کند. این جدول ها با استفاده از الگوریتم مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد منتشر می شوند. جدول های عضو کلاستر بوسیله ی گروه ها به روز می شوند. در این نوع پروتکل نود ها به دسته هایی تقسیم بندی می شوند. هر گروه یک سردهسته دارد که می تواند گروهی از میزبان ها را کنترل و مدیریت کند. از جمله قابلیت هایی که عمل دسته ای فراهم می کند می توان به اختصاص پهنای باند و دسترسی کانال اشاره کرد. این پروتکل از مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد به عنوان پروتکل مسیریابی زیر بنایی خود استفاده می کند. نیز در این نوع هر نود دو جدول یکی جدول مسیریابی و دیگری جدول مربوط به عضویت در نود های مختلف را فراهم می کند. معایب: نودی که سردهسته واقع شده سربار محاسباتی زیادی نسبت به بقیه دارد و به دلیل اینکه بیشتر اطلاعات از طریق این سردهسته ها برآورده می شوند در صورتی که یکی از نود های سردهسته دچار مشکل شود کل و یا بخشی از شبکه آسیب می بیند.

#### ۴-۳-۱-۱-۴ پروتکل مسیریابی تطبیقی درخت منبع STAR<sup>۱</sup>

این پروتکل نیاز به به روز رسانی مداوم مسیر ها نداشته و هیچ تلاشی برای یافتن مسیر بهینه بین نود ها نمی کند. در این پروتکل ترافیک اتصالات به دلیل تشکیل شدن مسیرهای غیر بهینه کاهش یافته است و استفاده بهتری از پهنای باند می کند که به دو صورت مسیریابی بهینه با کوتاهترین مسیر (ORA) و با کم ترین هزینه (LORA) پیاده سازی می شود.

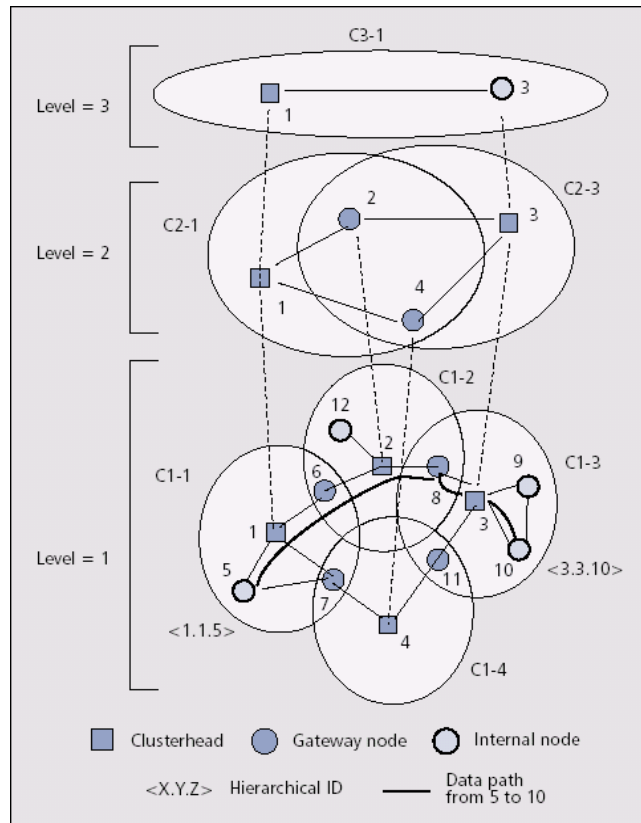
#### ۴-۳-۱-۱-۵ مسیریابی حالت سلسله مراتبی HSR<sup>۲</sup>

ویژگی روش های مسیریابی حالت سلسله مراتبی دسته بندی چند سطحی و تقسیم بندی منطقی گره های متحرک است، شبکه به دسته ها تقسیم بندی شده و یک سردهسته با یک الگوریتم انتخاب سردهسته برگزیده میشود. در این پروتکل این سردهسته ها از این پس خودشان را در دسته سازماندهی می کنند. گره های یک دسته اطلاعات لینک خود را به یکدیگر پخش می کنند. سردهسته اطلاعات کلاستر خود را خلاصه کرده و به سردهسته های همسایه از طریق دروازه ارسال می کند. همچنان که در شکل ۴-۳ نشان داده شده این سردهسته ها عضو کلاستری در یک سطح بالاتر هستند و اطلاعات لینک های خود را مطابق اطلاعات خلاصه شده سطح پائین تر بین یکدیگر رد و بدل می کنند. یک گره در هر سطح اطلاعاتی را که بعد از اجرای الگوریتم در آن سطح بدست آورده بصورت سیل آسا به سطح پائین تر خود ارسال می کند. سطح پائین تر هم اطلاعات توپولوژی سلسله

1- source tree adaptive routing

2 Hierarchical State Routing

مراتبی دارد. هر گره یک آدرس سلسله مراتبی دارد، یک راه برای متناظر کردن آدرس سلسله مراتبی شماره دسته با شروع از ریشه به آن گره مطابق شکل ۳-۴ می باشد.



شکل ۳-۴ یک نمونه سلسله مراتب در روش HSR

یک دروازه توسط ریشه از طریق یک، چند مسیر قابل دسترسی است، بطوریکه دروازه میتواند یک یا چند آدرس سلسله مراتبی داشته باشد. یک آدرس سلسله مراتبی برای تحویل از هر جای شبکه به میزبان کافی می باشد. بعلاوه گره ها همچنین به زیر شبکه های منطقی تقسیم بندی شده اند و هر گره به یک آدرس منطقی متناظر شده است. هر زیر شبکه یک سرور مدیر محلی (LMS) دارد، همه گره های زیر شبکه آدرس منطقی خود را با سرور مدیر محلی ثبت می کنند و او هم آدرس سلسله مراتبی آنها را به سطوح بالاتر اعلام کرده و اطلاعات همچنین برای تمام سرورهای مدیر محلی هم پایین فرستاده می شود. لایه انتقال بسته ای را با آدرس منطقی مقصد به لایه شبکه می فرستد، لایه شبکه آدرس سلسله مراتبی سرور مدیر محلی مقصد را از سرور مدیر محلی خودش بدست می آورد و سپس بسته را به آن میفرستد و سرور مدیر محلی مقصد بسته را به مقصد ارسال می کند. چونکه از این پس مبدا و مقصد آدرس سلسله مراتبی همدیگر را می دانند می توانند سرور مدیر محلی را کنار گذاشته و خودشان مستقیماً برای هم ارسال کنند. از آنجائیکه آدرس منطقی / آدرس سلسله مراتبی برای مسیریابی استفاده می شود برای نقل انتقالات شبکه هم می تواند تطبیق پذیر باشد.

#### ۴-۳-۱-۲ پروتکل های واکنشی (بر حسب تقاضا)

این نوع مسیریابی با مسیریابی بر حسب جدول یک تفاوت کوچک دارد. در این روش مسیر گزینی انجام می شود و این عمل زمانی صورت می پذیرد که گره اصلی (ریشه) وجود داشته باشد. هنگامی که یک گره به مسیریابی به سوی یک مقصد نیاز دارد، این مسیر بوسیله پردازش در شبکه به صورت مخفی انتخاب می شود و این روش مسیریابی همه ی مسیرهای ممکن را از مبدأ به مقصد امتحان می کند. هر مسیری تنها یک بار پخش می شود تا اینکه کوتاهترین مسیر انتخاب شود. در این نوع پروتکل مسیرها تنها زمانی کشف می شوند که مبدأ اقدام به برقراری ارتباط با نود دیگری کند. زمانی که یک نود بخواهد با نود دیگری ارتباط برقرار کند بایستی فرایند کشف مسیر<sup>۱</sup> را در شبکه فراخوانی کند. در این حالت قبل از برقرار شدن ارتباط، تاخیر قابل توجهی مشاهده می شود. این دسته از پروتکل ها را بر مبنای طلب درخواست مبداء بنا نهاده اند. برخی از این پروتکل ها عبارتند از:

#### ۴-۳-۱-۲-۱ پروتکل مسیریابی پایداری (ثبات) سیگنال SSR<sup>۲</sup>

این پروتکل مسیرها را بر مبنای قدرت و توان سیگنالها بین نود ها انتخاب می کند. بنابراین مسیرهایی که انتخاب می شوند نسبتاً قوی تر هستند. می توان این پروتکل را به دو بخش پروتکل مسیریابی پویا<sup>۳</sup> و پروتکل مسیریابی ایستا<sup>۴</sup> تقسیم کرد. قسمت پویا مسئول تهیه و نگهداری جدول مسیریابی و جدول مربوط به توان سیگنال ها می باشد. قسمت ایستا نیز بسته های رسیده را بررسی می کند تا در صورتی که آدرس نود مربوط به خود را داشته باشد آن را به لایه های بالاتر بفرستد و در غیر این صورت به شبکه.

#### ۴-۳-۱-۲-۲ پروتکل مسیریابی از مبداء پویا DSR<sup>۵</sup>

در این نوع پروتکل نود های موبایل بایستی cache هایی برای مسیر هایی که از وجود آنها مطلع هستند فراهم کنند. دو فاز اصلی برای این پروتکل در نظر گرفته شده است، کشف مسیر و به روز رسانی مسیر. فاز کشف مسیر از بسته های درخواست مسیر و پاسخ مسیر و فاز به روز رسانی مسیر از بسته های تصدیق دریافت و خطاهای لینکی استفاده می کند. جدول از قبل تهیه شده و فقط به همان مسیرهایی که برایش مشخص شده است می تواند دسترسی داشته باشد. این پروتکل از مسیریابی مبداء استفاده می کند.

#### ۴-۳-۱-۳ پروتکل مسیریابی منظم زمانی TORA<sup>۶</sup>

- 1- Route Discovery Process
- 2 - Signal Stability Routing
- 3 - Dynamic Routing Protocol
- 4 - Static Routing Protocol
- 5 - Dynamic Source Routing protocol
- 6 - Temporally-Ordered Routing Algorithm

بر اساس الگوریتم مسیریابی توزیع شده بنا شده و برای شبکه های موبایل بسیار پویا طراحی شده است. این الگوریتم برای هر جفت از نود ها چندین مسیر تعیین می کند و نیازمند clock سنکرون می باشد. یک پروتکل مسیریابی توزیعی توسط مبداء می باشد که اطلاعات کنترلی را محدود می کند. ۳ عمل اصلی این پروتکل عبارتند از: ایجاد مسیر. به روز رسانی یا نگهداری مسیر و از بین بردن مسیر. یک الگوریتم مسیریابی بسیار قابل تطبیق، موثر، قابل توسعه و توزیع شده بر مبنای مفهوم معکوس لینک است. در واقع یک پروتکل مبتنی بر تقاضا است به این معنی که گره مبداء قبل از ارسال بسته یک مسیریابی انجام می دهد و تا زمانی که به مسیر نیاز نباشد مسیری ایجاد نمی گردد. این پروتکل برای شبکه های بی سیم متحرک بسیار پویای چندگامی پیشنهاد شده است. این نوع پروتکل برای بارگذاری با ترافیک پایین و تحرک به صورت م یانه مناسب است زیرا در صورت تحرک بالا ممکن است روش ارسال بسته ها ی داده به صورت انتخابی صورت گیرد نه سریل آسا. 'DAG یک گراف غیرچرخشی است که گره ها آن را در طول ایجاد مسیر و فاز نگهداری برای هر مقصد ایجاد می کنند. مسیریابی از هر نودی در گراف می تواند شروع شود و به یک مقصد توسط لینک های مستقیم به شرح ذیل ارسال گردد:

قابلیت تطبیق بالا- کارآمد- مقیاسی و الگوریتم توزیع شده مسیرهای چندگانه از منبع به مقصد.

در این پروتکل به هر گره یک سطح میزان مرجع اختصاص می یابد. در این پروتکل زمانبندی یک عامل مهم است، زیرا ارتفاع (درجه یا همان گامها از یک گره به مقصد) به زمان منطقی خراب شدن یک لینک وابسته است. پیکربندی مسیر یکنواخت است و بروزرسانی مسیرهای متناوب نیازی نیست. این نوع پروتکل که شامل مسیریابی واکنشی است در بسیاری از کاربردهای شبکه های سربار، عملکرد بهتری نسبت به الگوریتم های متری بر جدول دارد. این پروتکل مسیریابی از نوع مسیریابی واکنشی می باشد و استفاده از گراف های غیرگردشی مستقیم در جایی که هر گره مسیری به یک مقصد معین دارد را میسر می سازد.

هر گره یک ۵ تایی دارد که از اجزا زیر تشکیل شده است:

۱- زمان منطقی خراب شدن لینک (T)

۲- شناسه یکتای گره ای که در سطح ارجاعی جدید تعیین شده است (oid)

۳- یک بیت نشان دهنده انعکاس (r)

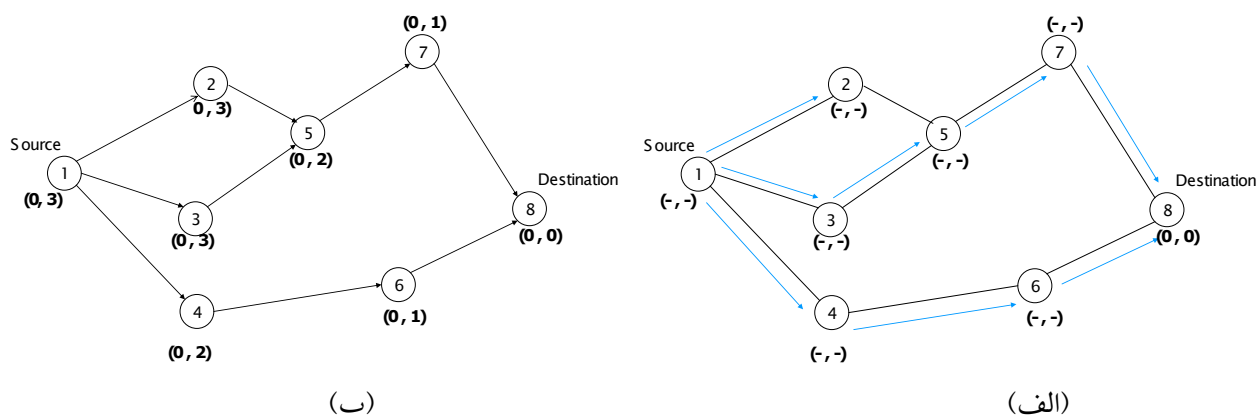
۴- یک پارامتر سفارش دهی انتشار (height)

۵- شناسه جاری یکتای خود گره (i)

سه المان اول جمعا سطح ارجاع را بیان میکنند یک سطح ارجاع جدید هر زمان که یک گره لینک ورودی خود را بسته به یک خرابی از دست بدهد رخ میدهد. دو مقدار آخر یک دلتا را با توجه به سطح ارجاع تعریف می کنند.

#### ۴-۳-۱-۳-۲-۱ ایجاد مسیر

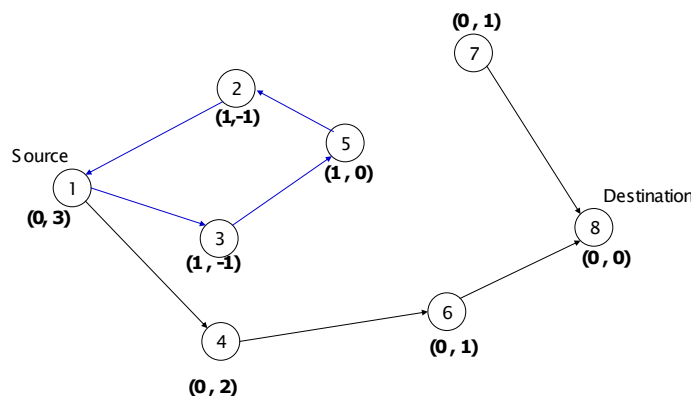
الگوریتم ایجاد مسیر با استفاده از بسته های QRY و UPD انجام می گیرد. به این صورت که گره مبدا درخواست مسیر (بسته QRY) را به صورت (شناسه گره، -، -، -) تنظیم کرده و به گره های مجاور خود پخش می کند و هر گره نیز آن را به گره های مجاور خود ارسال می کند تا این بسته به مقصد برسد و در انتها گره مقصد بسته UPD را به صورت (شناسه گره، تعداد گام گره جاری تا مقصد، ۰، ۰، ۰) تنظیم کرده و به گره های مجاور خود به صورت معکوس ارسال کرده تا این بسته به مبدا رسیده و مسیر مشخص شود و به روز رسانی گردد. الگوریتم ایجاد مسیر با ارتفاع مقصد که به مقدار صفر تنظیم شده و ارتفاع سایر گره ها که مقدار تهی دارد آغاز می شود، مبدا یک بسته QRY را با استفاده از شناسه گره مقصد که در آن بسته قرار داده شده است برای همه همسایه ها پخش می کند، یک گره با یک ارتفاع غیر تهی با یک بسته UPD پاسخ می دهد که مقدار ارتفاع در آن قرار دارد. گرهی که UPD را دریافت میکند مقدار ارتفاع خود را با یک مقدار بیشتر از گرهی که UPD را تولید کرده تنظیم میکند. گره با ارتفاع بزرگتر به عنوان جریان بالا در نظر گرفته می شود و گره با ارتفاع کمتر بعنوان جریان پایین در نظر گرفته می شود. به این ترتیب یک گراف بدون حلقه مستقیم از مبدا تا مقصد ساخته میشود. شکل ۴-۴ یک رویه ساخت مسیر در این پروتکل را نشان می دهد. در این شکل در قسمت الف گره ۱ مبدا و گره ۸ مقصد است، گره ۱ پیغام های Query را برای همسایه هایش می فرستد و این عمل تکرار می شود تا گرهی که مسیری به مقصد دارد با یک ارتفاع پاسخ دهد.



شکل ۴-۴ نمونه ای از مکانیزم ایجاد مسیر در TORA

همچنان که در شکل ۴-۴ قسمت الف نشان داده شده گره پنج از گره سه هیچ گزارش منتشر شده ای را دریافت نمی کند چون قبلاً از گره دو دریافت کرده است. در شکل قسمت ب مبداء (مثلاً گره ۱) ممکن است یک بسته UPD از گره دو یا گره سه دریافت کند، ولی از آنجایی که گره چهار مقدار ارتفاع کمتری را ارائه می دهد آن را پذیرفته و ارتفاع آنرا حفظ می کند. وقتی که گره حرکت می کند و تغییر مکان می دهد مسیر DAG شکسته می شود و به نگهداری مسیر برای ایجاد دوباره یک DAG برای همان مقصد نیاز است. وقتی که آخرین لینک جریان پایین یک گره خراب می شود یا سطح مرجع جدید را تولید می کند، این باعث انتشار سطح مرجع گره ها با همسایه ها مثل شکل ۴-۵ می شود.

لینک ها برای بازتاب تغییر در بازیابی ها برای سطح مرجع جدید برگشت داده می شود (معکوس می شوند). این ممکن است تاثیر مشابهی در معکوس کردن در جهت یک یا چند لینک، زمانی که یک گره لینک جریان پایین ندارد داشته باشد. در فاز پاک کردن مسیر، این پروتکل بسته های پاک کردن را روی شبکه برای از بین بردن مسیرهای نامعتبر پخش می کند.



شکل ۴-۵ نگهداری مسیر در TORA

در این پروتکل پتانسیل رخ دادن نوسانات وجود دارد بخصوص وقتی چندین مجموعه از هماهنگ کردن گره ها بطور همزمان عملیات تشخیص تکه تکه شدن شبکه، پاک کردن مسیر و ساخت مسیرهای جدید بر مبنای یکدیگر ایجاد شود. چون در این پروتکل هماهنگی بصورت میان گرهی انجام می شود مشکل بی ثباتی و نوسان آن شبیه مشکل حلقه بی نهایت در پروتکل های بردار مسافت است، با این تفاوت که برخی نوسانات زود گذر هستند و همگرایی در نهایت اتفاق می افتد.

#### ۴-۳-۲-۱-۳-۲ نگهداری مسیر

این عمل زمانی انجام می گیرد که یک لینک از بین برود و در این حالت سه پارامتر  $(t, oid, r)$  به روز رسانی شده و به گره های مجاور ارسال می گردد تا آنها نیز از خرابی مسیر مطلع شوند.  $t$  نشان دهنده زمانی است که

لینک خراب شده ، oid شناسه گره ای است اکنون در سطح ارجاع قرار دارد و  $r$  که بیت انعکاس است مقدار ۱۰ می گیرد که ۰ نشان دهنده گره اصلی و ۱ نشان دهنده گره انعکاس داده شده می باشد . اگر لینکی از بین برود که هنوز گره ها مسیری به مقصد داشته باشند مشکلی ایجاد نمی شود.

۱- تولید کردن : زمانی که لینک یک گره از بین می رود ، این گره در سطح ارجاعی جاری قرار گرفته و یک سطح جدید ایجاد می کند و ۳ پارامتر اول را تنظیم کرده و در یک بسف UPD آن خرابی را به گره های همسایه اطلاع می دهد تا گره مبداء در جریان قرار گیرد در این حالت یک معکوس سازی کامل صورت می گیرد یعنی گره ای که در سطح ارجاعی جاری قرار گرفته تمام لینک های خود را معکوس می کند.

۲- منتشر کردن : زمانی که گره های همسایه گره سطح ارجاعی جاری بسف UPD را دریافت می کنند سطح ارتفاع یا همان پارامتر را از طریق فرمول

$$dj: \text{ where neighbor } j \text{ has the highest first three elem} \} - 1 \} \min = d \text{ set}$$

تنظیم کرده و یک معکوس سازی جزئی را انجام می دهند یعنی گره لینک های خود را به جز لینکی که بسف UPD را از آن دریافت کرده معکوس می کند.

۳- منعکس کردن : زمانی که گره ای بسف upd را دریافت می کند ، ۳ پارامتر اول  $(t, Oid, r)$  گره های همسایه خود را مقایسه کرده که اگر یکسان باشند مقدار پارامتر  $r$  را به ۱ و مقدار پارامتر  $t$  را به ۰ تنظیم می کند .

۴- کشف کردن : در این قسمت بخشی از مسیر به مقصدی که از بین رفته یافت شده ، در واقع به گره ای می رسیم که لینک مسیر از آنجا خراب شده ( به گره سطح ارجاعی جاری رسیدیم)

#### ۴-۳-۲-۱-۳-۴ پاک کردن مسیر

زمانی که مبداء از خرابی لینک مطلع شد شروع به پاک کردن مسیر و ارسال بسته CLR به سمت گره ای که از آنجا خرابی رخ داده می شود که در این حالت پارامتر  $r$  برابر ۱ شده که نشان دهنده پاک کردن مسیر است.

#### ۴-۳-۲-۱-۳-۴ الگوریتم های مورد استفاده در TORA

این پروتکل ترکیبی از دو الگوریتم LMR و GB است که در ذیل شرح داده می شوند:

الگوریتم LMR<sup>۱</sup>: این الگوریتم مبتنی بر تقاضا بوده که در شبکه های موبایلی استفاده می شود و پای و اساس آن معکوس سازی لینک است و همچنین مسیریابی را که در زمان ارسال بسف QRY (درخواست کشف مسری) و بسف UPD (به روزرسانی) مورد نیاز است را مشخص می نماید ، البته تنها زمانی که کشف مسری از طرف گره



منع درخواست گردد و می تواند در زمان خرابی لینک با معکوس سازی لینک های گره جاری و ارسال بسته upd گره های همسایه را آگاه نماید.

الگوریتم GB<sup>1</sup>: در شبکه ممکن است بخشی از مسیری به مقصد بنا به دلایلی از بین برود که این باعث بروز ناپایداری شبکه می شود، این الگوریتم به هر گره یک ارتفاع منحصر به فرد را اختصاص می دهد و می تواند ناپایداری شبکه را تشخیص دهد و در این زمان یک مقدار ارتفاع جدید برای گره ها در نظر می گیرد و از طریق پخش بسته UPD گره های شبکه را از زمان خرابی لینک مطلع می سازد.

این پروتکل توسط LMR می تواند کشف مسیری کرده و معکوس سازی لینک را در زمان خرابی لینک انجام دهد و از طریق GB می تواند تعداد گام هر گره را نسبت به مقصد تشخیص دهد و هنگام از بین رفتن یک لینک از زمان آن مطلع شده و مقدار ارتفاع (گام) جدیدی در نظر گرفته و با پخش بسته upd در شبکه، گره ها را مطلع نماید.

#### ۴-۳-۱-۲-۳-۵ معایب پروتکل TORA

(۱) چون عملکردها به ارتباط گره ها واکنش نشان می دهند، سرریزی در زمان کشف مسیری و اصلاح مسیری رخ می دهد.

(۲) نمی تواند مسیری های کوتاه را اولویت بندی کند.

یکی از معایب پروتکل این است که نمی تواند مسیری های کوتاه را اولویت بندی کرده و بهترین مسیری را تشخیص دهد و در هنگام کشف مسیری، بسته QRY را به تمام گره های همسایه ارسال می کند که باعث ایجاد سربار می شود. حال اگر بتوان این پروتکل را به گونه ای تنظیم نمود که بتواند بهترین گره را در بین گره های همسایه تشخیص داده و بسته QRY را تنها برای آن گره بفرستد، می توان سرباری را که در هنگام کشف مسیری ایجاد می شود را کاهش داده و زمان کمتری صرف می شود. مثلاً می توان برای هر گره وزنی در نظر گرفت (همان طول عمر گره) و بسته QRY را به گره ای که طول عمر بیشتری دارد ارسال کرد.

#### ۴-۳-۱-۲-۳-۶ خواص پروتکل TORA

(۱) نگهداری مسیری از طریق لینک معکوس

دلیلی این کار، پیدا کردن مسیری جایگزین برای زمانی است که مسیری اصلی از بین می رود.

(۲) دارای قابلیت تطبیق بالا و سریع برای ایجاد مسیری در زمان از بین رفتن لینک مقصد می باشد.

۳) کشف مسیری به صورت سراسری می باشد یعنی می توان با ارسال درخواست مسیریابی تمام گره ها، مسیری مناسب را کشف نمود.

۴) این پروتکل ویژگی منحصر به فردی در نگهداری مسیریابی چند گانه به مقصد دارد.

#### ۴-۳-۱-۲-۴ پروتکل مسیریابی مبتنی بر شرکت پذیری<sup>۱</sup> ABR

میزان پایداری اتصالات در مسیر را محاسبه می کند .

#### ۴-۳-۱-۲-۵ پروتکل مسیریابی بردار مسافت بر حسب تقاضا<sup>۲</sup> AODV

این پروتکل مسیریابی براساس الگوریتم مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد که قبلاً توضیح داده شده است پیاده سازی می شود. این پروتکل حالت پیشرفته ی DSDV می باشد. زیرا این پروتکل نیز به دنبال کوتاهتر کردن مسیرها می باشد. هنگامی که یک گره بخواهد پیغامی را به گره مقصد که مستقیماً مسیری به سوی آن ندارد بفرستد ، درخواست مسیر را برای همسایه هایش آماده کرده و می فرستد تا اینکه پیغام با یک یا چند واسطه بوسیله ی یک مسیر تازه به مقصد می رسد. در طول مراحل پیشروی بسته درخواست مسیر، گره های واسطه آدرس همسایه ها را بوسیله کپی کردن در جدول مسیریابی ثبت می کند تا اینکه یک مسیر معکوس از مقصد به مبدأ تولید کند که اصطلاحاً به این مسیر معکوس، مسیر پاسخگوی درخواست مسیر گفته می شود. این مسیر پاسخگو برای اعلام و تصدیق رسیدن پیغام به مقصد استفاده می شود. این پروتکل فقط اتصال های سیستماتیک را ساپورت می کند و به دلیل مسیریابی تنها در زمان نیاز میزان پخش بسته ها را کاهش می دهد .

#### ۴-۳-۱-۲-۶ میکرو تفاوت (تنوع جزئی) مسیریابی فاصله نسبی<sup>۳</sup> RDMAR

این نوع از پروتکل فاصله ی بین دو گره را از طریق حلقه های رادیویی و الگوریتم های فاصله یابی محاسبه می کند. این پروتکل محدوده ی جستجوی مسیر را مقدار مشخص و محدودی تعیین می کند تا بدین وسیله از ترافیک ناشی از سیل آسا در شبکه کاسته باشد .

#### ۴-۳-۱-۳ پروتکل های ترکیبی - پیوندی ( بر حسب جدول و بر حسب تقاضا )

این مورد با ترکیب دو روش قبلی سعی در کاهش معایب کرده و از ویژگی های خوب هر دو مورد بهره می برد. این پروتکل جدید ترین کلاس پروتکل ها در این راستا می باشد. معروفترین پروتکل از این نوع می توان به

1 -Associativity Based Routing Protocol

2 - Ad hoc On-demand Distance Vector routing protocol

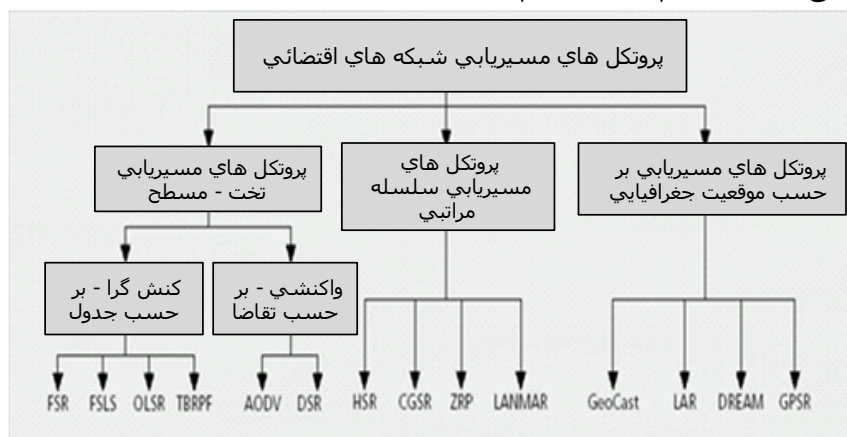
3 - Relative Distance Micro diversity Routing

ZRP اشاره کرد. این پروتکل از ویژگی های نوع فعال برای مسیریابی نود های نزدیک به هم و از ویژگی های نوع واکنشی برای مسیریابی نود های دورتر استفاده می کند .

#### ۴-۳-۱ پروتکل مسیریابی ناحیه ای ZRP<sup>۱</sup>

نوعی از دسته بندی است با این تفاوت که در این پروتکل هر نود خود سر بوده و به عنوان عضوی از بقیه ی دسته ها می باشد. به دلیل ترکیبی بودن کارایی بهتری دارد .

#### ۴-۳-۲ پروتکل های تقسیم بندی دوم



شکل ۴-۶ طبقه بندی پروتکل های مسیریابی در شبکه های اقتضائی

همان طور که در شکل نشان داده شده است، پروتکل های مسیریابی در شبکه های اقتضائی به سه دسته عمده تقسیم می شوند:

#### ۴-۳-۲-۱ پروتکل های مسیریابی تخت (سطح)

در این پروتکل ها یک سطح مسیریابی وجود دارد و این پروتکل ها به دو دسته عمده بر حسب جدول و بر حسب تقاضا دسته بندی می شوند. پروتکل های ترکیبی که تلفیقی از دو حالت اصلی هستند نیز موجود می باشند.

#### ۴-۳-۲-۱-۱ پروتکل های تخت فعال (بر حسب جدول)

این پروتکل ها مبتنی بر جدول مسیریابی می باشند و دائماً مسیرها را مورد بازبینی قرار می دهند و آنها را به روز می نمایند. این پروتکل ها در مسیریابی تاخیری ندارند ولی ظرفیت زیادی را برای مدیریت جداول مسیریابی استفاده می نمایند. نمونه ای از این پروتکل ها OLSR<sup>۲</sup> و TBRPF<sup>۳</sup> می باشد.

#### ۴-۳-۲-۱-۲ پروتکل های تخت واکنشی (بر حسب تقاضا)

1 - Zone Routing Protocol

2 - Optimized Link State Routing protocol

3 - Topology-Based Reverse Path Forwarding

در این پروتکل های مسیریابی یافتن مسیر به صورت بر حسب تقاضا صورت می پذیرد و مسیرها دائماً به روز نمی شوند. گلوگاه این مسیریابی ها در تاخیر اولیه برای یافتن مسیر به سمت مقصد می باشد و لذا این پروتکل ها برای مقاصد بلادرنگ مناسب نیستند. از سوی دیگر این پروتکل ها در استفاده از انرژی و پهنای باند بهینه عمل می کنند. نمونه ای از این پروتکلها DSR و AODV می باشد.

#### ۳-۱-۲-۳-۴ پروتکل های تخت ترکیبی

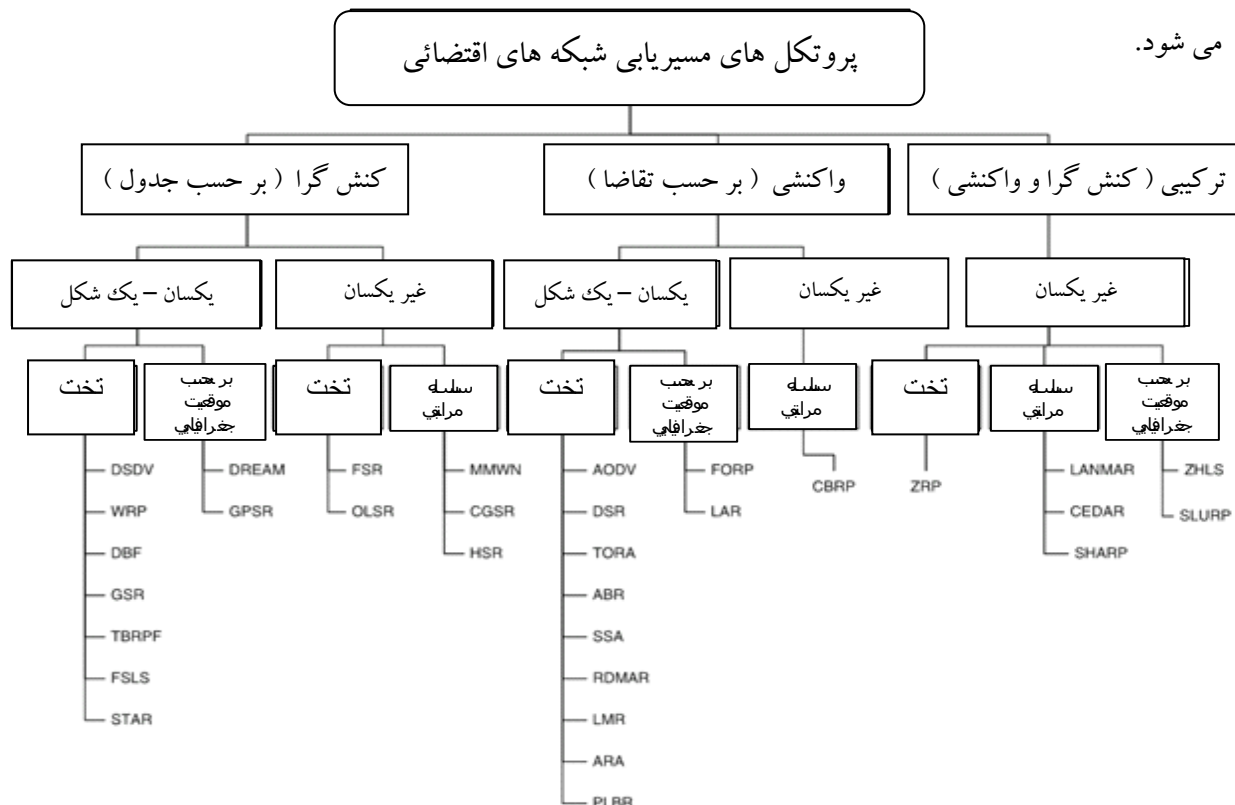
این پروتکل ها در هر دو حالت کنش گرا و واکنشی می توانند عمل نمایند. نمونه ای از این پروتکل ها TORA می باشد.

#### ۲-۲-۳-۴ پروتکل های مسیریابی سلسله مراتبی

وقتی ابعاد شبکه توسعه پیدا می کند پروتکل های مسیریابی تخت دیگر جوابگو نمی باشند و نیاز به استفاده از پروتکل های مسیریابی سلسله مراتبی می باشد. این پروتکل ها بر این اساس کار می کنند که با دسته بندی نودها در قالب گروهها به آنها عملکردهای متفاوتی تخصیص داده می شود.

#### ۳-۲-۳-۴ پروتکل های مسیریابی مبتنی بر موقعیت جغرافیائی

در این پروتکل های مسیریابی به جای استفاده از آدرس مقصد برای مسیر یابی از موقعیت جغرافیائی آن استفاده می شود.



شکل ۷-۴ طبقه بندی نسبتاً جامع پروتکل های مسیریابی در شبکه های اقتضائی

حال در ادامه به بررسی کامل تر الگوریتم های مسیریابی AODV و DSR و OLSR می پردازیم .

#### ۴-۴ پروتکل مسیریابی از مبدا پویا<sup>۱</sup>

پروتکل مسیریابی از مبدا پویا جزو روش های شناخته شده مسیریابی شبکه های اقتضائی متحرک می باشد، این پروتکل یک پروتکل واکنشی است که می تواند شبکه های اقتضائی را بدون نیاز به جداول مسیریابی و به روز سازی آنها مدیریت کند. این پروتکل به طور اخص برای شبکه های اقتضائی چند پرشه<sup>۲</sup> طراحی می شود. به منظور صرفه جویی در پهنای باند فرایند مسیریابی تنها زمانی انجام می شود که نیاز باشد (مقتضی). در این پروتکل فرستنده تمام مسیرهای منبع به مقصد را مشخص و آدرس تمام گره های میانی را در بسته ها ذخیره می کند. این پروتکل بر مبنای الگوریتم های موقعیت پیوند<sup>۳</sup> کار می کند یعنی هر گره قادر به ذخیره ی بهترین مسیر به مقصد است. همچنین اگر تغییری در شبکه رخ دهد تمام گره های شبکه از طریق انتشار کلی (سیل آسا) از این تغییر مطلع می شوند. این پروتکل شامل دو مکانیزم که با هم برای کشف و نگهداری مسیر های مبدا در شبکه اقتضائی کار می کنند ترکیب شده است.

##### ۴-۴-۱ کشف مسیر

کشف مسیر در پروتکل مسیریابی از مبدا پویا به اینصورت انجام میشود که مبدا S بسته ای را برای مشخص کردن مقصد D ایجاد می کند، در هر بسته یک مسیر شامل گام هایی که بسته باید از آنها برای رسیدن به مقصد D عبور کند را قرار می دهد. S یک مسیر مبدا مناسب را با جستجو در حافظه موقت مسیر خود (که شامل مسیر هایی است که از قبل میداند) بدست می آورد ولی اگر مسیری در حافظه اش به این مقصد پیدا نکرد پروتکل "کشف مسیر" را برای پیدا کردن پویای یک مسیر به مقصد D آغاز می کند، که S آغاز کننده و D هدف کشف مسیر است.

##### ۴-۴-۲ نگهداری مسیر

نگهداری مسیر مکانیزمی است که برای نگهداری و بازسازی مسیرهای مورد استفاده بکار می رود. در حالیکه یک مسیر از مبدا S به مقصد D مورد استفاده است توپولوژی شبکه ممکن است تغییر کند (این حرکت گره ها و تغییر مداوم توپولوژی، ماهیت شبکه های اقتضائی است) بطوریکه گره مبدا دیگر نتواند مسیر به مقصد را استفاده کند بدلیل اینکه یک لینک در طول مسیر به مقصد ممکن است دیگر کار نکند. وقتی روال نگهداری مسیر نشان

1 -Dynamic Source Routing Protocol (DSR)

2 - multi hop

3 - link state

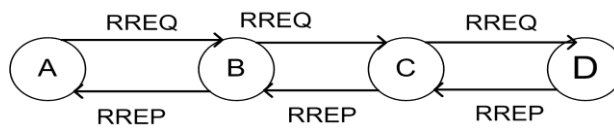
می دهد که یک مسیر مبدا شکسته شده است، S می تواند تلاش کند که مسیر دیگری را که بلد است یعنی در حافظه نهان خود دارد برای ارسال به D استفاده کند و یا اینکه دوباره مکانیزم کشف مسیر را بکار ببرد تا یک مسیر جدید کشف کند. مکانیزم نگهداری مسیر فقط زمانی استفاده می شود که S واقعا در حال ارسال بسته ها به D باشد. هر دو مکانیزم کشف مسیر و نگهداری مسیر کاملاً بصورت بر حسب تقاضا کار می کنند، در واقع بر خلاف بسیاری از پروتکل های دیگر شبکه اقتضائی در روش پروتکل مسیریابی از مبدا پویا هیچ نوع بسته ای در هیچ سطحی بصورت دوره ای در شبکه ارسال نمی شود و این رفتار بر حسب تقاضا و کمبود فعالیت های دوره ای باعث کم شدن بسته های سر بار می شود. در پاسخ به یک کشف مسیر یکتا یک گره چندین مسیر را به یک مقصد یافته و ذخیره می کند. این باعث می شود که عکس العمل نسبت به تغییرات مسیر یابی بسیار سریع شود، از آنجائیکه اگر مسیر مورد استفاده با خرابی مواجه شد مسیر دیگری را مورد استفاده قرار می دهد، در ضمن این ذخیره کردن چند مسیر باعث می شود که از سر بار مورد نیاز برای اجرای یک کشف مسیر جدید زمانی که مسیر مورد استفاده خراب می شود جلوگیری شود. عملیات های کشف و نگهداری مسیر در این پروتکل طوری طراحی شده اند که توسط هر دو نوع لینک یک طرفه و لینک های متقارن پشتیبانی می شوند. این پروتکل می تواند ارتباط بین گره های با شعاع های متفاوت را پشتیبانی نماید، بعلاوه مسیر یابی این پروتکل بر مبنای مسیر یابی استاندارد اینترنت است که یک گره دروازه هم به اینترنت متصل است و هم عضوی از گره های در گیر در پروتکل مسیریابی شبکه اقتضائی می باشد. همچنین با مسیریابی IP متحرک هم سازگار است که یک گره دروازه نقش یک عامل خارجی IP متحرک را انجام می دهد.

در این پروتکل تمامی مسیرهای فرا گرفته شده توسط یک نود در حافظه نهان<sup>1</sup> آن ذخیره می شود. این حافظه نهان ممکن است چندین مسیر به سمت مقصد را در خود ذخیره کرده باشد. هر مسیر ذخیره شده یک زمان انقضایی دارد و پس از آن از حافظه نهان حذف می شود. اگر یک نود میانی پیغام درخواست مسیر<sup>2</sup> دریافت کند و در حافظه نهان خود به سمت مقصد مسیری داشته باشد، بدون اینکه این پیغام درخواست مسیر را منتشر کند، مسیر به مقصد را در پاسخ ارسال می نماید. نودهای میانی نیز که مکرراً پیغامهای درخواست مسیر و پاسخ مسیر<sup>3</sup> را می شنود می توانند این مسیرها را ذخیره نمایند. این پروتکل یک پروتکل مسیریابی بر حسب مبداء می باشد و لذا هر بسته اطلاعات تمامی مسیر از مبداء تا مقصد را با خود حمل می کند.

1 - Cache

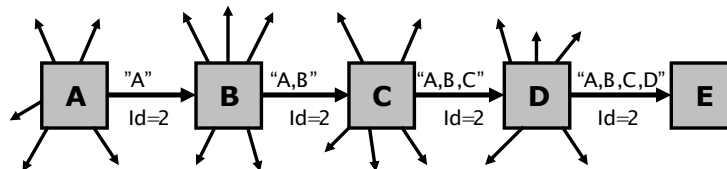
2 - Route Request (RREQ)

3 - Route Reply (RREP)

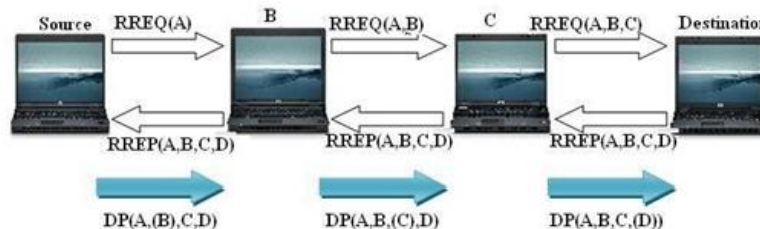


شکل ۴-۸ پیغامهای درخواست مسیر و پاسخ مسیر برای مسیریابی

در شکل ۴-۹ یک مثال از کشف مسیر توضیح داده شده است، گره A تلاش می کند که یک مسیر به گره E بدست آورد، برای آغاز مکانیزم کشف مسیر گره A یک پیغام درخواست مسیر بصورت یک بسته فراگیر به همه گره هایی که در محدوده ارسالش هستند می فرستد، هر بسته درخواست مسیر گره آغاز کننده و گره هدف کشف مسیر را مشخص کرده و هم چنین حاوی رکوردی از لیست هر گره میانی است که یک کپی از پیغام درخواست مسیر به آن ارسال شده است این رکورد با یک لیست خالی توسط آغاز کننده کشف مسیر مقدار دهی اولیه می شود و هر گرهی که آنرا دریافت می کند نام خود را به آن اضافه میکند.



شکل ۴-۹ مکانیزم کشف مسیر در پروتکل مسیریابی از مبدا پویا: گره A سعی در بدست آوردن مسیری به E دارد



شکل ۴-۱۰ کشف مسیر در پروتکل مسیریابی از مبدا پویا از گره A تا D (DP: Data Packet)

وقتی گره دیگری درخواست مسیر را دریافت می کند اگر خودش گره مقصد باشد یک پیغام پاسخ مسیر را به آغاز کننده کشف مسیر بر می گرداند، یک کپی از رکورد لیست گره های مسیر انباشته شده بر می دارد و این مسیر را در حافظه مسیریابی برای ارسال متوالی بسته ها به این مقصد ذخیره می کند، در حالت دیگر یعنی اگر خودش مقصد نباشد اگر گرهی که درخواست مسیر را دریافت می کند قبلاً بسته ای با شناسه (ID) یکسان با این بسته دریافت کرده و یا خودش در رکورد لیست مسیر های انباشته، این بسته را دارد، آنرا دور می ریزد و گرنه آدرس خود را به آن اضافه کرده (در رکورد مسیر در پیغام درخواست مسیر) و آنرا به صورت یک بسته فراگیر محلی ارسال می کند (با شناسه درخواست یکسان). در بازگرداندن پاسخ مسیر به آغاز کننده کشف مسیر، مثلاً از E به A در شکل ۴-۹ معمولاً حافظه مسیر خود را بررسی خواهد کرد که بیند آیا مسیری به A وجود دارد و اگر بود آنرا برای برگرداندن پاسخ مسیر به گره A مورد استفاده قرار می دهد، در غیر این صورت

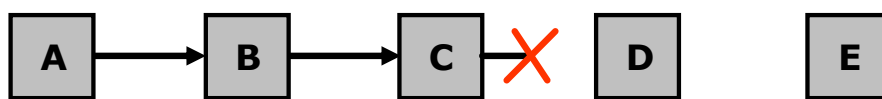
گره E ممکن است برای پیدا کردن گره A یک مکانیزم کشف مسیر را استفاده کند ولی برای اجتناب از بازگشت نامتناهی احتمالی کشف مسیر ها باید این پاسخ مسیر را روی درخواست مسیر A سوار کند و برگرداند، حتی می توان بسته های داده کوچک دیگر مثل بسته TCP-SYN را روی بسته درخواست مسیر با استفاده از یک مکانیزم مشابه سوار کرد. گره E می تواند به سادگی زنجیره گام های ثبت شده در لیست مسیر را معکوس کند و سعی کند پاسخ مسیر را روی آن بفرستد و این مسیر را برای حمل بسته پاسخ مسیر خود استفاده کند. پس از آغاز یک کشف مسیر فرستنده بسته یک کپی از بسته اصلی را در یک بافر محلی به نام بافر ارسال ذخیره می کند، بافر ارسال حاوی یک کپی از هر بسته ای است که نتوانسته توسط این گره ارسال شود زیرا تا کنون مسیر از مبداء ای را برای ارسال به مقصد بسته ها نداشته است. هر بسته در بافر ارسال با زمان جاگذاری در بافر برچسب می خورد و بعد از ماندن در بافر به مدت دوره انقضای زمانی دور انداخته می شود. اگر لازم شود که از سرریز شدن بافر جلوگیری شود از استراتژی ورودی اول خروجی اول<sup>۱</sup> یا استراتژی دیگری می تواند برای خارج کردن بسته ها قبل از انقضای زمان آنها استفاده شود. اگر یک بسته در بافر ارسال قرار دارد گره باید گاه و بیگاه یک کشف مسیر جدید را برای آدرس مقصد بسته ها انجام دهد.

#### ۴-۳-۴ اصول نگهداری مسیر در پروتکل مسیریابی از مبدا پویا

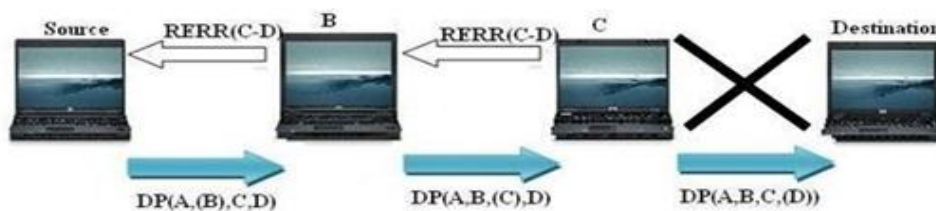
وقتی که یک بسته با استفاده از یک مسیر مبدا ارسال شد هر گره ای که بسته را انتقال می دهد باید مطمئن شود که بسته بوسیله گام بعدی در طول مسیر دریافت شده است یعنی تصدیق و تأیید رسیدن بسته را دریافت کند. به عنوان مثال در شکل ۴-۹ گره A یک بسته را برای گره E با استفاده از مسیر مبدا و از طریق گره های میانی B, D, C ارسال کرده است در این حالت گره A مسئول است که رسید دریافت بسته را توسط B دریافت کند و B مسئول است که رسید دریافت را توسط C دریافت کند و بقیه هم تا مقصد به همین صورت عمل می کنند، این تأیید دریافت در بسیاری از موارد ممکن است بدون هیچ هزینه ای در این پروتکل انجام شود چه به عنوان یک قسمت استاندارد از پروتکل MAC ای که استفاده می شود (مثل فریم های تصدیق سطح لینک که بوسیله IEEE... تعریف شده) و چه با یک تصدیق دریافت غیر فعال (مثلا B تأیید را در C با گوش فرا دادن به ارسال C، زمانی که C بسته را برای فرستادن به D روی خط ارسال می کند دریافت کند). اگر هیچ کدام از این دو مکانیزم آماده نبود گره احتمالاً بسته را با تنظیم کردن یک بیت در هر بسته برای درخواست یک تصدیق نرم افزاری ویژه پروتکل مسیریابی از مبدا پویا که برگشت داده شود تحویل گره بعدی می دهد. اگر لینک بین دو



گره یک جهته باشد این تصدیق نرم افزاری ممکن است روی مسیر دیگری که حتی شاید شامل چندین گام باشد برگردانده شود. اگر گره به اندازه ما کزیم تعداد بار ممکن بسته را ارسال کند ولی تائیدی دریافت نکند یک پیغام خطای مسیر برای فرستنده اصلی ارسال می شود به نشانه این که یک لینک در روی مسیر نمی تواند عمل ارسال را انجام دهد. به عنوان مثال در شکل ۴-۱۱ اگر C نتواند به خاطر شکستگی لینک، بسته را به D تحویل دهد، یک پیغام خطای مسیر به A بر می گرداند. گره ها این مسیر شکسته شده را از حافظه خود پاک می کنند، اگر A در حافظه اش مسیر دیگری به E داشته باشد بسته را با استفاده از این مسیر جدید فوراً ارسال می کند و گرنه ممکن است یک کشف مسیر جدید برای این هدف انجام دهد.

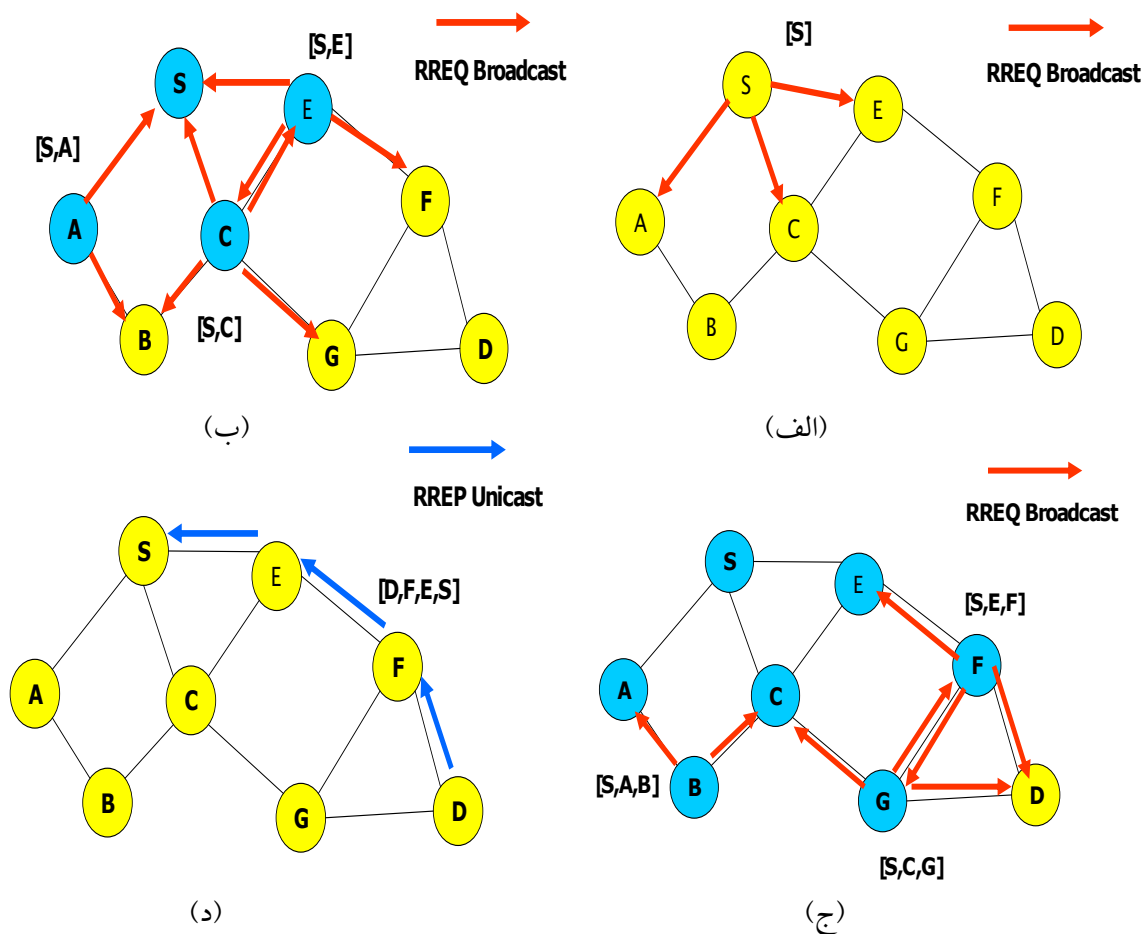


شکل ۴-۱۱ نمونه ای از نگهداری مسیر در DSR که گره C قادر به ارسال بسته A به E نیست



شکل ۴-۱۲ نگهداری مسیر در پروتکل مسیریابی از مبدا پویا (DP: Data Packet)

**مثال:** شکل ۴-۱۳ را در نظر بگیرید، فرض کنیم گره S میخواهد بسته ای را برای گره D ارسال نماید و در حافظه اش مسیری از قبل آماده به D ندارد، بنا براین مکانیزم کشف مسیر را آغاز میکند، همانطور که در شکل ۴-۱۳ قسمت الف مشاهده می شود، گره S یک بسته درخواست مسیر به همسایه های مستقیمش، یعنی A, C و E ارسال میکند که در هدر آن یک لیست خالی مسیر نیز قرار داده میشود، هر یک از این گره ها با دریافت بسته چون که خودشان مقصد نیستند و نیز مسیر مستقیمی به مقصد هم ندارند نام خود را به بسته اضافه نموده و آنرا برای همسایه های مستقیم شان ارسال مینمایند که در شکل ۴-۱۳ قسمت ب نشان داده شده است، همانطور که در این شکل مشاهده میشود بعضی از گره ها مثل E و C ممکن است دو بار یا بیشتر یک بسته درخواست مسیر را دریافت کنند، که در اینصورت آنرا دور می اندازند.



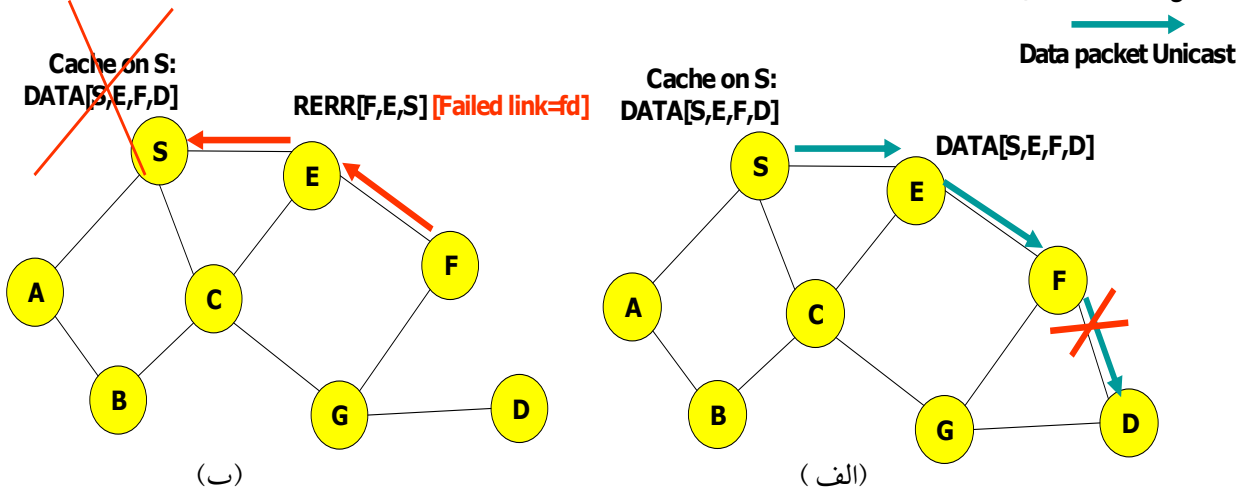
شکل ۴-۱۳ نمونه ای از مکانیزم کشف مسیر در پروتکل مسیریابی از مبدا پویا

عمل ارسال به همسایه ها تا زمانیکه یک گره یا خودش مقصد باشد و یا راهی به مقصد داشته باشد ادامه پیدا میکند و در مرحله سوم به B و سپس در مرحله چهارم به گره های F و G میرسد که هر دوی آنها مسیری به مقصد D دارند، بنابراین پیغام پاسخ مسیر روی همان مسیری که پیغام درخواست مسیر آمده برگردانده می شود، مثلاً از مسیری که در شکل ۴-۱۳ قسمت د نشان داده شده است، ذکر این نکته ضروری است که مبدا S ممکن است چندین پاسخ مسیر را دریافت کند در اینصورت از بین آنها بهترین مسیر را که می تواند کوتاهترین مسیر باشد انتخاب کرده و بقیه مسیرها را در جدول مسیر یابیش (در حافظه اش) ذخیره می کند تا اگر مسیر جاری دچار شکستگی لینک شد و خراب شد از آنها برای جایگزینی آن استفاده نماید.

حال فرض کنید که لینک گره F به گره D دچار شکستگی شده است و دیگر قابل استفاده نیست در اینصورت گره F این شکستگی مسیر را فهمیده و برای اینکه متوجه این خرابی لینک شود یک پیغام خطا را به طرف مبدا از همان مسیر برعکس ارسال می فرستد و گره مبدا یعنی S با دریافت این پیغام خطا در حافظه اش تمام مسیرهایی را که شامل این لینک هستند حذف میکند و اگر به غیر از آنها مسیر دیگری وجود داشت که از طریق آنها ارسال می کند و اگر نه دوباره یک مکانیزم کشف مسیر جدید را آغاز می کند تا مسیر تازه ای را به مقصد

گره D پیدا کند و دوباره داده را به آن ارسال نماید. این فعل و انفعالات در شکل ۴-۱۴ الف و شکل ۴-۱۴ ب

نشان داده شده است.



شکل ۴-۱۴ فاز نگهداری مسیر در پروتکل مسیریابی از مبدا پویا

#### ۴-۴-۴ مزایای پروتکل مسیریابی از مبدا پویا

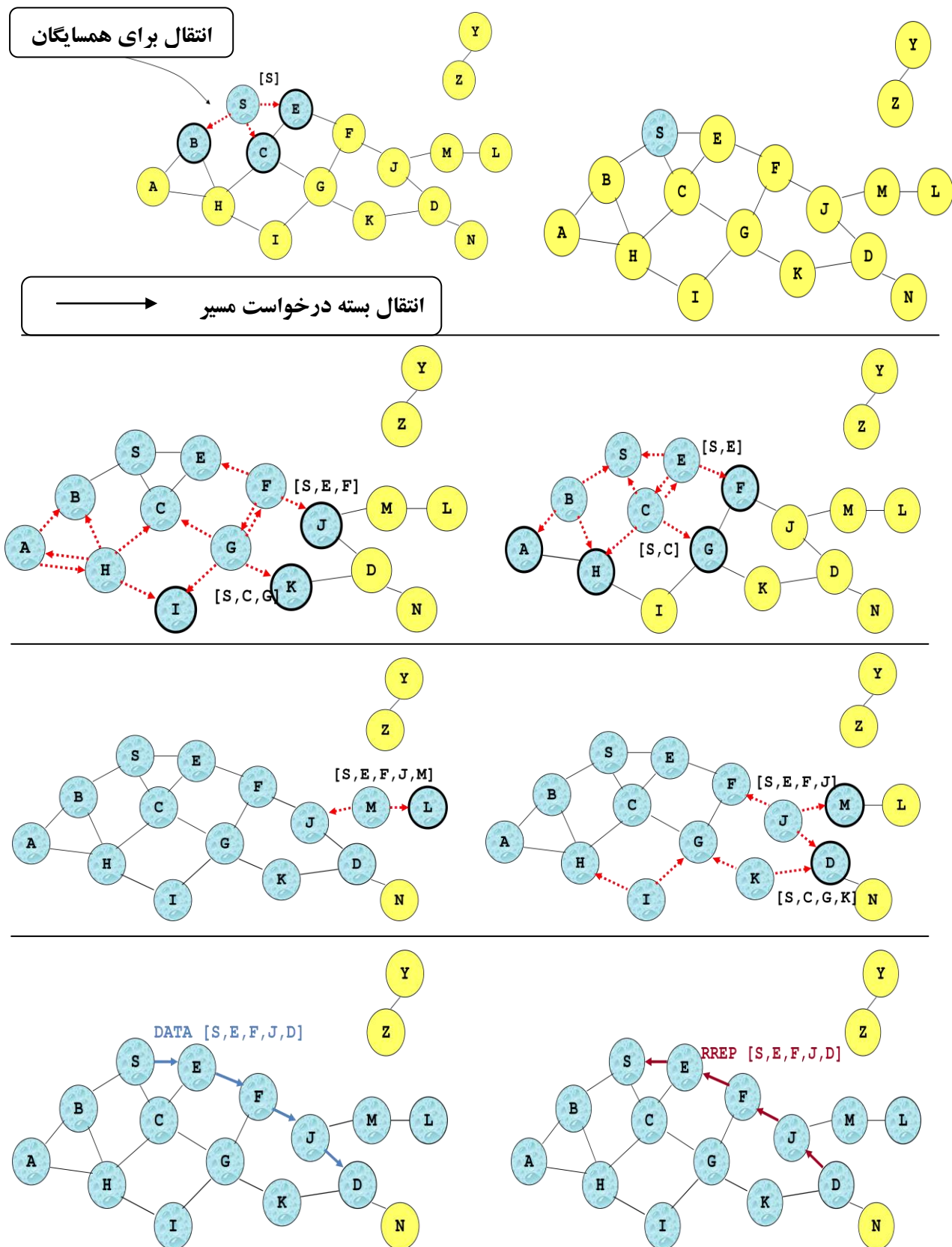
- (۱) ترافیک کلی مسیریابی در کل شبکه پایین می باشد.
- (۲) در سناریوهایی که تحرک در آنها وجود دارد به خوبی کار می کند.
- (۳) به سرعت به خرابی لینک پاسخ می دهد.

#### ۴-۴-۵ معایب پروتکل مسیریابی از مبدا پویا

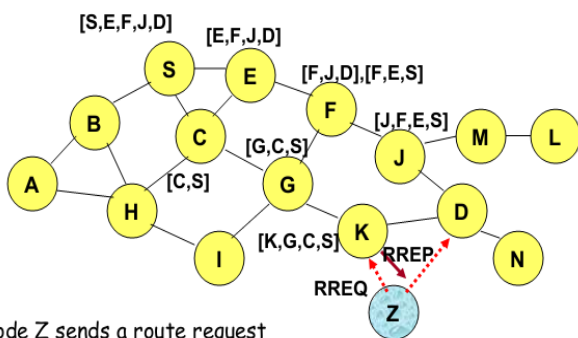
- (۱) بسته های داده تا زمان پیدا شدن مسیر می بایستی بافر بشوند.
- (۲) این پروتکل به علت اضافه شدن اطلاعات مسیر در بسته های داده مقیاس پذیر نمی باشد.
- (۳) ممکن است در کاربردهای بلادرنگ غیر قابل استفاده باشد.

#### ۴-۴-۶ یک مثال از پروتکل مسیریابی از مبدا پویا

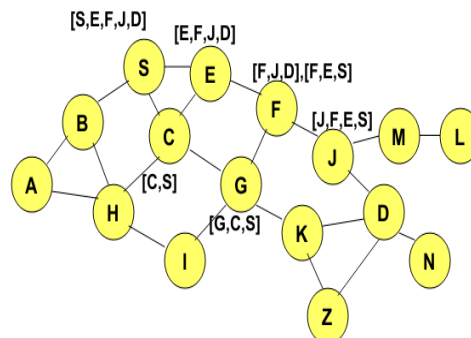
در شکل های صفحه بعد یک مثال مسیریابی از گره S تا D در پروتکل مسیریابی از مبدا پویا (ارسال بسته های درخواست مسیر و دریافت بسته پاسخ مسیر و ارسال داده) را می توانید مشاهده نمایید.



شکل ۴-۱۵ مسیریابی از گره S تا D در پروتکل مسیریابی از مبداء پویا (ارسال بسته های درخواست مسیر و دریافت بسته پاسخ مسیر و ارسال داده)

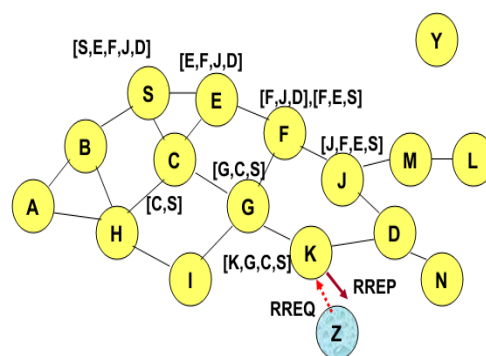
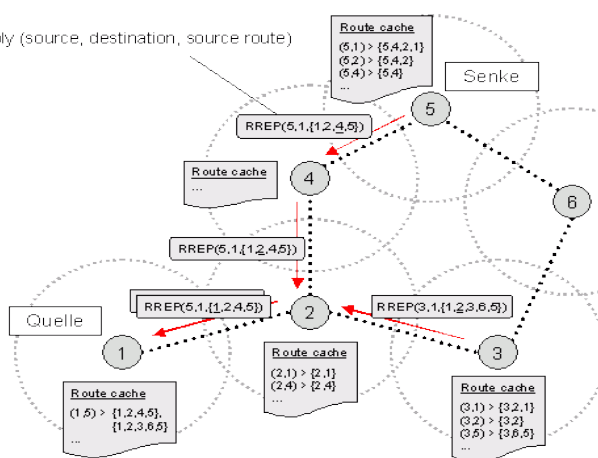


When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route



[P,Q,R] Represents cached route at a node  
(DSR maintains the cached routes in a tree format)

Route reply (source, destination, source route)



□ Route Reply (RREP) from node K limits flooding of RREQ.

شکل ۴-۱۶ مثال از کاربرد حافظه نهان نودها در پروتکل مسیریابی از مبداء پویا

## ۴-۵ پروتکل مسیریابی بردار مسافت بر حسب تقاضا اقتضائی<sup>۱</sup>

این پروتکل در سال ۱۹۹۹ پیشنهاد شده است و با به کارگیری بسیاری از ویژگی های پروتکل مسیریابی از مبداء پویا سعی کرده است پروتکل مسیریابی بردار مسافت بر مبنای شماره ترتیب مقصد (معرفی در سال ۱۹۹۷) را به یک پروتکل بر حسب تقاضا تبدیل نماید. این پروتکل نمونه ای از یک پروتکل مسیریابی بر حسب نیاز است که بر اساس مسیر یاب بردار فاصله عمل می کند. محدودیت پهنای باند و طول باطری را در این محیط در نظر می گیرد. در آن همه مسیرها فقط وقتی که مورد نیاز باشند کشف می شوند و تنها در طول مدتی که مورد استفاده قرار می گیرند نگهداری می شوند. مسیرها در طول یک سیل آسا کشف می شوند که در طی آن نودهای شبکه در فرآیند جستجوی یک مسیر به سمت مقصد مورد سوال قرار می گیرند. وقتی یک نود با یک مسیر به مقصد کشف می شود آن مسیر به عقب و به نود مبدائی که درخواست مسیر کرده بود گزارش می شود. این پروتکل

برای شبکه هایی با چند ده تا چند صد گره طراحی شده است. یکی از جنبه های این پروتکل استفاده از شماره ی رشته (توالی) در جدول هر گره است. این شماره رشته توسط گره مقصد تولید می شود، شماره ی رشته هم در بسته درخواست مسیر و هم در بسته های پاسخ به مسیر گنجانده می شود و به گره های درخواست کننده فرستاده می شود. شماره رشته از اهمیت فوق العاده ای برخوردار است. زیرا باعث اجتناب از حلقه شده و به سادگی قابل برنامه ریزی است. در دیگر گره ها نیز این شماره رشته به منظور به روز رسانی اطلاعات مسیر یابی استفاده می شود. اگر یک گره بین دو مسیر حق انتخاب داشته باشد مسیری را انتخاب می کند که شماره رشته آن بیشتر باشد. این پروتکل با جداول مسیریابی سازگار است. بسته های درخواست مسیر، جواب به مسیر و خطا در این پروتکل نیز همانند پروتکل مسیریابی از مبداء پویا تعریف می شود. عمل مسیریابی در هر نود به صورت مستقل انجام می شود، بنابراین هیچ مسیریابی در مبداء انجام نمی گیرد. از آنجایی که درخواست مسیر و پاسخ مسیر به صورت پرودیگ ارسال و دریافت نمی شوند برای مطلع شدن از شکسته شدن لینک این پروتکل مانند پروتکل مسیریابی از مبداء پویا از مکانیزم خطا در مسیر استفاده می نماید و مانند پروتکل مسیریابی از مبداء پویا اگر نودی متوجه شکسته شدن لینک گردد پیغام خطا در مسیر را در مسیر برگشت تا نود مبداء می فرستد.

این پروتکل برای تحقق اهداف زیر طراحی شده است:

حداقل سربار کنترلی

حداقل سربار پردازشی

قابلیت مسیریابی چندگامی

نگهداری پویای توپولوژی

عاری بودن از حلقه

چون منابع در شبکه های متحرک اقتضائی کم طلب هستند این پروتکل سعی می کند تا سربار کنترلی را با محدود کردن بروزرسانی های متناوب مسیری و همچنین تنها استفاده از پیغام های بر حسب تقاضا به حداقل برساند. برای به حداقل رساندن سربار پردازشی، پیغام های این پروتکل ساختار ساده ای دارند و فقط به محاسبات کمی دارند. در یک شبکه اقتضائی منابع و مقصدها ممکن است در خارج از محدوده ارتباطی مستقیم یکدیگر باشند که این به خاطر محدودیت حوزه ارسال توجهات میسر است. از این رو این پروتکل نودها را قادر می سازد بتوانند از کشف مسیریابی چندگامی به سمت مقصد استفاده کنند و این مسیریابی ها را تا وقتی که توپولوژی شبکه به طور مدام تغییری می کند نگهداری کنند. همچنین در برابر حلقه های مسیریابی به شدت مقابله می کنند چون آنها در هر

شبکه ای پر هزینه هستند مخصوصا در یک شبکه بزرگ که ظرفیت سرگنالینگ و توان پردازشی نود محدود است. این پروتکل شامل دو فاز می باشد:

(۱) کشف مسیر

(۲) نگهداری مسیر

#### ۴-۵-۱ کشف مسیر

شبکه موقتی را در هر لحظه می توان به وسیله گرافی از گره ها (مسیریاب ها + میزبانها) توصیف کرد. دو گره در صورتی متصل به هم هستند که بتوانند مستقیما با استفاده از رادیوهای خود با یکدیگر ارتباط برقرار کنند (در این صورت در گراف یالی بین آنها وجود دارد). چون ممکن است یکی از آنها خیلی قوی تر از دیگری باشد ممکن است A به B متصل باشد اما B به A متصل نباشد. اما برای سهولت فرض می کنیم تمام اتصالات متقارن هستند. توجه داشته باشید که اگر دو گره در رادیوی یکدیگر باشند به معنای این نیست که به هم متصل هستند. این پروتکل انواع پیغام های زیر را تعریف می کند:

(۱) درخواست مسیر

(۲) پاسخ مسیر

(۳) خطای مسیر<sup>۱</sup>

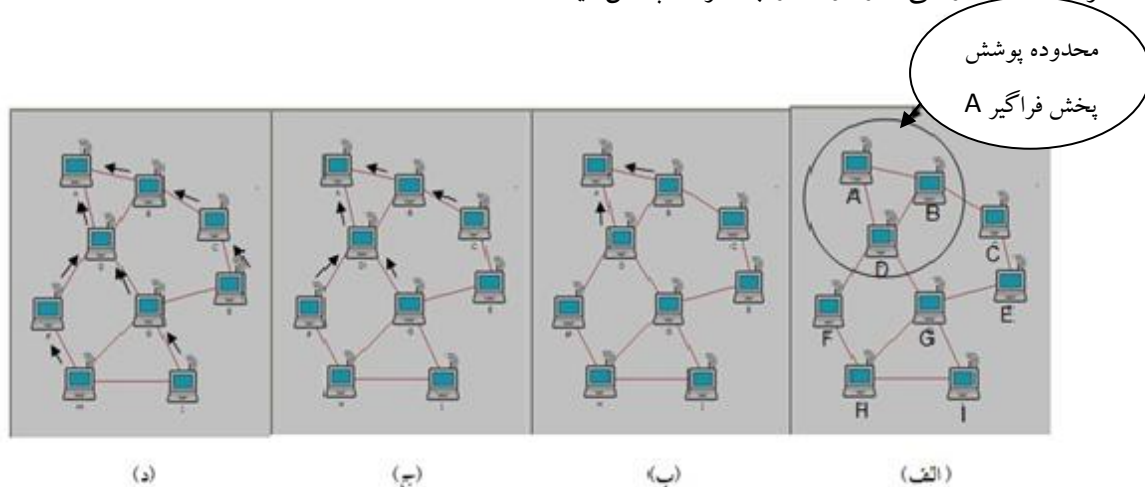
(۴) پاسخ مسیر همراه تصدیق دریافت<sup>۲</sup>

این پروتکل فرآیند پیدا کردن مسیر را با استفاده از بسته های درخواست مسیر انجام می دهد، در هر فرایند ارسال و دریافت درخواست مسیر و پاسخ مسیر، تنها نودهای قرار گرفته در مسیر این بسته ها مشخص می شوند و در اصل باعث به روز شدن بردار فاصله بین مبدا و مقصد می گردند. وقتی یک نود مبدأ نیاز به یک مسیر به یک نود مقصد داشته باشد و مسیر معتبری در جدول مسیریابی نباشد، نود مبدأ یک بسته درخواست مسیر را به سمت نود مقصد همه پخش می کند. وقتی هر نود درخواست مسیر را دریافت می کند، یک ورودی مسیر برعکس به سمت نود مبدأ را در جدول مسیریابی ایجاد یا بروزرسانی می کند و اگر یک مسیر معتبر در جدول مسیریابی به سمت نود مقصد ندارد، درخواست مسیر را دوباره همه پخش می کند. وقتی بسته سیل آسا درخواست مسیر از

1- Route Error (RERR)

2 -RREP-ACK

نود مبدأ به نود مقصد برسد، نود مقصد ورودی مسیر برعکس را ایجاد یا بروزرسانی می کند و یک بسته پاسخ مسیر را که یک شماره ترتیب افزایش یافته دارد در مسیر برعکس تک پخشی می کند. وقتی پاسخ مسیر به نود مبدأ و در طول مسیر برعکس می رسد، یک مسیر رو به جلو را به سمت مقصد ایجاد یا بروزرسانی کرده و ارتباطات شروع می شود. برای توصیف این الگوریتم شبکه موقتی شکل ۴-۱۷ را در نظر بگیرید که در آن فرایندی در گره (A) می خواهد بسته ای را به گره (I) بفرستد. ابتدا گره مبدأ (A) بسته درخواست مسیر خود به گره مقصد (I) را می سازد و آن را به اطراف پخش میکند.



شکل ۴-۱۷ نمایی از پروتکل مسیریابی AODV

سپس هر گره ای که در شعاع رادیویی گره مبدأ باشد (گره های B و D. علت این که B, D در گراف به A وصل هستند این است که A می تواند با آنها ارتباط برقرار کند. به عنوان مثال از F به A یالی وجود ندارد زیرا نمی تواند سیگنال رادیویی A را دریافت کند. لذا F به A وصل نیست). بسته درخواست مسیر را شنود می کند و اگر بسته تکراری باشد، آنگاه آن را دور می ریزد و اگر تکراری نباشد، به جدول مسیر خود نگاه می کند. اگر مسیر تازه ای به مقصد درخواستی در جدول موجود باشد، آنگاه بسته جواب مسیر را می سازد و برای گره مبدأ در یک جهت پخش می کند. ولی اگر مسیر تازه ای وجود نداشت، آنگاه به شمارنده گره یک واحد می افزاید، بسته درخواست مسیر را دوباره به همه گره های همسایه پخش می کند و اطلاعات مبدأ را برای مسیریابی معکوس ذخیره می کند. الگوریتم این پروتکل در هر گره دارای جدولی است که کلید آن مقصد است و اطلاعاتی راجع به آن مقصد ارائه می کند. B, D نمی دانند I در کجا قرار دارد، لذا هر کدام از آنها وارد ای را برای مسیر معکوس ایجاد می کنند که به A اشاره می کند (مثل فلش های شکل ۴-۱۷) بسته را در حالی پخش می کنند که فیلد شماره جهش آن ۱ است. پخش حاصل از B به D و C می رسد. C وارد ای را در جدول مسیر معکوس خود ایجاد می کند و آن را پخش می کند در حالی که D آن را بعنوان پخش تکراری رد می کند. به طور مشابه



پخش حاصل از D توسط B رد می شود. پخش D توسط F, G پذیرفته و ذخیره می شود. (شکل ۴-۱۷ ج) پس از اینکه E, H, I پخش را دریافت کردند، درخواست مسیر به مقصدی می رسد که می داند I در کجا قرار دارد (یعنی خود I) شکل (۴-۱۷ د). البته باید به این نکته توجه کرد که پخش بسته ها به صورت هماهنگ نیستند.

#### ۴-۱-۵-۱ ساخت و پخش بسته درخواست مسیر توسط گره مبدا

فرمت بسته درخواست مسیر در شکل ۴-۱۸ آمده است. این فرمت حاوی آدرسهای منبع و مقصد (معمولا آدرس IP آنها) است که مشخص می کند چه کسی برای چه کسی جست و جو می کند. شناسه تقاضا یک شمارنده محلی است و توسط هر گره ای نگهداری می شود و هر وقت درخواست مسیر پخش می شود یک واحد به آن اضافه می شود فیلدهای آدرس منبع و شناسه تقاضا، یک بسته درخواست مسیر منحصر به فرد را مشخص می کنند که به گره ها اجازه می دهند بسته های تکراری را حذف کنند.

شمارنده جهش	شماره ترتیب مقصد	شماره ترتیب منبع	آدرس مقصد	شناسه تقاضا	آدرس منبع
-------------	------------------	------------------	-----------	-------------	-----------

شکل ۴-۱۸ قالب بسته درخواست مسیر

هر گره علاوه بر شمارنده شناسه تقاضا، شمارنده دنباله ای دارد که هر وقت درخواست مسیر فرستاده شد (یا پاسخی به درخواست مسیر داده شد) یک واحد به آن اضافه می شود. تقریبا مثل ساعت عمل می کند و برای تشخیص مسیر جدید از مسیر قدیم به کار می رود. فیلد چهارم در شکل ۴-۱۸ شماره ترتیب A است و فیلد پنجم جدیدترین مقدار شماره ترتیب I است که A آن را دیده است. فیلد شمارنده جهش مشخص می کند که بسته تا کنون چند جهش انجام داده است. مقدار اولیه آن صفر است. وقتی بسته درخواست مسیر به گره ای می رسد به صورت زیر پردازش می شود:

۱. دو فیلد (شناسه تقاضا و آدرس منبع) را در جدول خود جست و جو می کند تا مشخص شود آیا این درخواست قبلا دیده و پردازش شده یا خیر. اگر تکراری باشد، نادیده گرفته می شود و پردازش متوقف می گردد، اگر تکراری نباشد این فیلدها را در جدول خود قرار داده و پردازش ادامه می یابد.
۲. گیرنده مقصد را در جدول مسیر خود جست و جو می کند اگر مسیر تازه ای به مقصد شناخته شود. بسته پاسخ مسیر به منبع ارسال می شود تا به آن بگوید چگونه به مقصد برسد. معنای مسیر تازه این است که شماره ترتیب مقصد که در جدول مسیریابی ذخیره شده است بزرگتر یا مساوی شماره ترتیب مقصد موجود در بسته درخواست

مسیر است. اگر کمتر باشد مسیر ذخیره شده قدیمی تر از مسیر قبلی است که منبع برای مقصد داشته است در نتیجه مرحله ۳ اجرا می شود.

۳. چون گیرنده مسیر تازه ای به مقصد ندارد به فیلد شمارنده جهش یک واحد اضافه می کند و بسته درخواست مسیر را پخش می کند. داده ها را نیز از بسته استخراج و آن را بعنوان وارده جدید در جدول مسیر معکوس خود ذخیره می کند. این اطلاعات برای ساختن مسیر معکوس به کار می روند لذا پاسخ می تواند بعدا به منبع برسد. فلشها در شکل ۴-۱۷ برای ساخت مسیر معکوس به کار می روند. برای وارده مربوط به مسیر معکوس جدیدی که ساخته شد، تایمری شروع به کار می کند وقتی تایمر از کار افتاد وارده حذف می شود.

در پاسخ به تقاضای ورودی، I یک بسته پاسخ مسیر را می سازد (شکل ۴-۱۹) آدرس منبع و آدرس مقصد از تقاضای ورودی کپی می شوند، اما شماره ترتیب مقصد از شمارنده اش به حافظه منتقل می شود. فیلد شمارنده جهش برابر با صفر می شود. فیلد طول عمر مشخص می کند که مسیر چه مدت معتبر است. این بسته یک بسته تک پخش به گره ای است که بسته درخواست مسیر از آن آمده است که در اینجا G است. سپس مسیر معکوس را به D طی می کند و به A می رسد. در هر گره شمارنده جهش یک واحد اضافه می شود لذا گره می تواند تشخیص دهد که چقدر از مقصد I فاصله دارد.

طول عمر	شماره جهش	شماره ترتیب مقصد	آدرس مقصد	آدرس منبع
---------	-----------	------------------	-----------	-----------

شکل ۴-۱۹ قالب بسته پاسخ مسیر

در هر گره میانی در مسیر معکوس بسته بررسی می شود اگر یک یا چند شرط زیر برقرار شود آن گره به عنوان مسیری به I در جدول مسیریابی محلی ذخیره می شود:

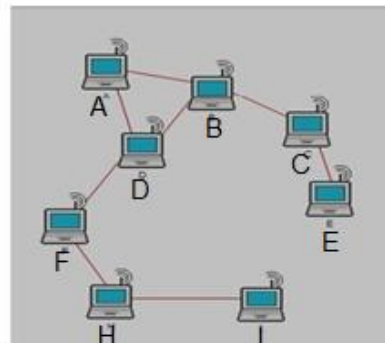
- هیچ مسیری به I شناخته نشده باشد
  - شماره ترتیب مربوط به I در بسته پاسخ مسیر بزرگتر از مقدار موجود در جدول مسیریابی است
  - شماره های ترتیب برابرند ولی مسیر جدید کوتاه تر است. (تشخیص از شمارنده جهش)
- بدین ترتیب تمام گره های موجود در مسیر معکوس مسیری به I به طور رایگان یاد می گیرند. گره هایی که بسته پاسخ مسیر را گرفتند ولی در مسیر معکوس نبودند (B, C, E, F, H در مثال ما)، با انقضای مدت تایمر مربوط، وارده ها را از جدول مسیر معکوس حذف می کنند. به علت انتشار زیاد بسته ها در شبکه می توان از فیلد

زمان زنده بودن<sup>۱</sup> در بسته IP استفاده نمود. با توجه به این فیلد، فرایند کشف مسیر را به این صورت می توان اصلاح نمود که برای یافتن مقصد، فرستنده یک بسته درخواست مسیر را می فرستد که فیلد زمان زنده بودن آن ۱ است. اگر در مدت زمان معقولی پاسخ دریافت نشود، بسته درخواست مسیر دیگری ارسال می شود. این بار فیلد زمان زنده بودن آن برابر با ۲ خواهد بود. دفعات بعد مقداری برابر با ۳ و ۴ و ۵ و غیره خواهد شد به این ترتیب جست و جو به طور محلی انجام می شود و به طور فزاینده فراگیرتر می شود.

#### ۴-۵-۲ نگهداری مسیر

چون گره ها می توانند جا به جا شوند یا خاموش شوند توپولوژی خود به خود تغییر می کند. بعنوان مثال در شکل ۴-۱۷ اگر G خاموش شود، A متوجه نمی شود که برای رسیدن به I مسیر (ADGI) را که استفاده می کرده دیگر معتبر نیست. الگوریتم باید این موضوع را اداره کند. هر گره به طور دوره ای پیام سلام<sup>۲</sup> می فرستد. انتظار می رود همسایه هایش به آن پاسخ دهند. اگر هیچ پاسخی دریافت نشود، پخش کننده متوجه می شود که همسایه ها از برد آن خارج شدند و دیگر به آن متصل نیستند. به طور مشابه، اگر سعی کند بسته ای به همسایه ای بفرستد و پاسخی دریافت نکند، متوجه در دسترس نبودن همسایه می گردد. این اطلاعات برای از بین بردن مسیرهایی به کار می روند که دیگر کار نمی کنند. هر گره مثل A، برای تک تک گره های مقصد که همسایه هایش در خلال  $\Delta T$  ثانیه گذشته بسته ای را از طریق او بدان مقصد ارسال کرده اند، فهرستی را نگه می دارد. این فهرستها را اصطلاحاً "همسایه های فعال A" می گویند. در این حالت گره A دارای جدولی است که کلید آن، آدرس مقصد گره های شبکه است. همچنین در این فهرست، گره بعدی برای رسیدن بدان مقصد، تعداد گام برای رسیدن به آن مقصد، آخرین شماره ترتیب و فهرست همسایه های فعال درج شده است. به عنوان مثال جدول مسیریابی گره D در مثال بالا چیزی شبیه به شکل ۴-۲۰ است.

فیلد های دیگر همسایه های فعال	فاصله	گام بعدی	مقصد
F, G	1	A	A
F, G	1	B	B
F	2	B	C
	2	G	E
A, B	1	F	F
A, B	1	G	G
A, B	2	F	H
A, B	2	G	I



شکل ۴-۲۰ (الف) گراف پس از حذف G از شبکه (ب) جدول مسیریابی D قبل از آن که G از کار بیفتد.

1 - TTL(Time To Live)

2 - Hello Message

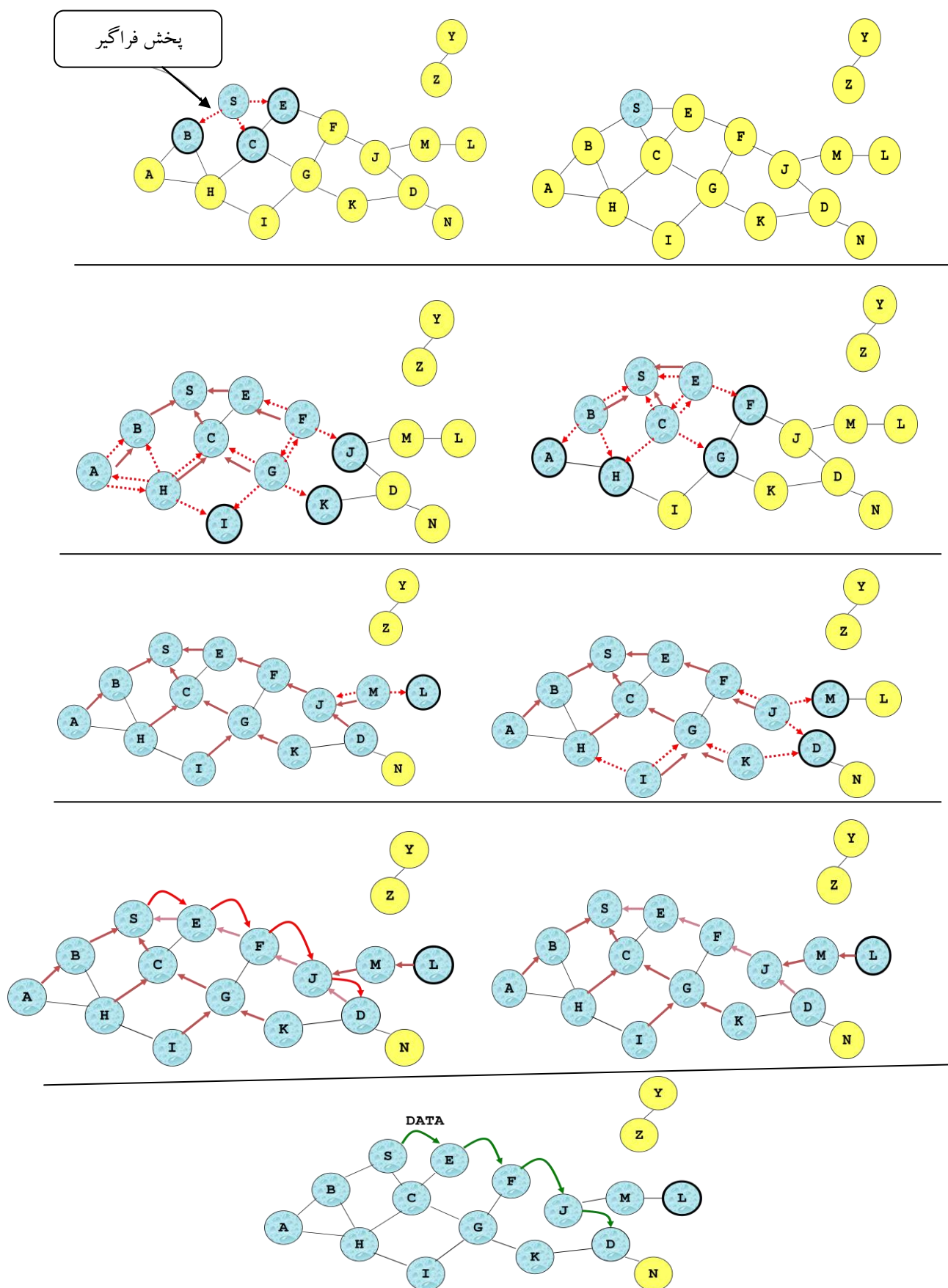
وقتی یکی از همسایه های A از دسترس خارج می شود، گره A جدول مسیریابی خود را بررسی می کند تا ببیند کدامیک از گره های شبکه در مسیرهای خود از گره حذف شده استفاده می کردند. این موضوع به همسایه های فعال اطلاع رسانی می شود که تمام مسیرهای آن ها از طریق A نامعتبر است. (چرا که N بسته های آن ها از طریق گره حذف شده ارسال می شده). همسایه های فعال نیز به همین منوال به همسایه های فعال خود اطلاع می دهند و این کار تکرار می گردد تا تمام مسیرهای وابسته به گره خارج از دسترس، از کل جدول های مسیریابی حذف شوند. به عنوان مثال در شکل ۴-۱۷ فرض کنید که گره G از دسترس خارج شده یا حذف شده (توپولوژی تغییر یافته در شکل ۴-۲۰)، وقتی گره D متوجه از بین رفتن گره G می گردد، به جدول مسیریابی خود نگاه می کند و می بیند که گره G بر روی مسیری قرار داشته که به E, G, I ختم می شده است. اجتماع مجموعه همسایه های فعال این سه گره مقصد عبارت است از  $\{A, B\}$ . به عبارت دیگر A, B در برخی از مسیرهای خود از گره G استفاده می کردند، لذا به این گره ها یا مسیریاب ها اطلاع داده می شود که دیگر گره G کار نمی کند. گره D به آن ها اطلاع رسانی می کند تا آن ها نیز جداول مسیریابی خود را اصلاح نمایند و خود گره D نیز درایه های متناظر با E, G, I را از جدول مسیریابی خود حذف می کند. تفاوت عمده بین این پروتکل و پلَمَن - فورد این است که در این پروتکل گره ها به طور تناوبی پخش هایی را که حاوی جدول های مسیریابی آنها باشد، انجام نمی دهند. بلکه بر حسب تقاضا، فقط بخشی از جدول ها که لازم است ارسال می گردد. این تفاوت منجر به صرفه جویی در پهنای باند و مصرف باتری می شود.

#### ۴-۵-۳ مزایای پروتکل مسیریابی بردار مسافت بر حسب تقاضا

- ۱) نودها تنها مسیرهایی را نگهداری می کنند که مورد نیاز می باشند.
- ۲) نیاز برای پخش فراگیر حداقل می شود.
- ۳) نیاز برای حافظه کم می شود.
- ۴) به از دست رفتن لینک های مسیر به سرعت پاسخ می دهد.
- ۵) از ایجاد حلقه در مسیر به صورت موثر جلوگیری می شود.
- ۶) این پروتکل برای تعداد نودهای بالا مقیاس پذیر می باشد.

#### ۴-۵-۴ یک مثال از پروتکل مسیریابی بردار مسافت بر حسب تقاضا

در شکل های زیر به ترتیب مراحل مسیریابی گره S تا گره D به وسیله این پروتکل (ارسال بسته های درخواست مسیر و دریافت بسته پاسخ مسیر و ارسال داده) را می توانید مشاهده نمایید.



شکل ۴-۲۱ یک مثال از پروتکل AODV - مسیریابی و ارسال داده از گره S تا گره D

## ۶-۴ پروتکل مسیریابی حالت پیوند بهینه<sup>۱</sup>

این پروتکل از دسته پروتکل های مسیریابی حالت لینک بشمار می رود . ایده مسیریابی حالت پیوند ساده است و در پنج بخش بیان می شود، هر مسیر یاب باید :

(۱) همسایه هایش را تشخیص داده و آدرس های شبکه آنها را بداند

(۲) تاخیر یا هزینه تا همسایه هایش را اندازه گیری کند

(۳) ایجاد بسته ای که گویای تمام اطلاعات بدست آمده باشد

(۴) این بسته ها را به تمام مسیر یابها ارسال کند

(۵) کوتاهترین مسیر به هر مسیر یاب دیگر را محاسبه کند

پروتکل مسیریابی حالت پیوند بهینه هم از این قوانین پیروی می کند . این پروتکل شامل چند مرحله است:

(۱) تولید بسته های کنترلی

(۲) ارسال بسته ها به دیگر نودها

(۳) ساخت درخت کوتاهترین مسیر (از طریق الگوریتم دایج کسترا)

(۴) تولید جدول مسیریابی

در این پروتکل ابتدا نقاط ارسال یا انتقال دهنده چند نقطه ای<sup>۲</sup>، شناسایی می شوند . این نقاط تنها نقاطی هستند

که در شبکه اجازه پخش اطلاعات را دارند و باعث کاهش سربار شبکه و کاهش ارسال بسته های کنترلی می

شوند اولین کار این پروتکل این است که همسایه هایش را شناسایی کند که این کار را با ارسال بسته سلام به

همسایه های اطراف هر نود انجام می دهد از این طریق هر نود نودهای اطرافش را شناسایی می کند . با اطلاعات

بدست آمده ، هر نود برای خودش جدولی درست می کند که ارتباط نود با همسایه هایش درون جدول قرار دارد

. در مرحله بعد هر کدام از نودها اطلاعات خود به همراه شماره ترتیب را در قالب بسته کنترل توپولوژی<sup>۳</sup> برای

نودهای اطراف می فرستد البته انتقال بسته های کنترل توپولوژی تنها از طریق نودهای ارسال چند نقطه ای انجام

می شود. به این طریق تمام نودهای موجود در شبکه از اتصالات موجود و نحوه ارتباط با هر نود آگاهی

دارند. اطلاعات مربوطه در قالب جدولی برای هر نود ذخیره می شود . در مرحله بعد هر نود از اطلاعات جمع

آوری شده باید بهترین مسیر به هر نود را انتخاب کند . انتخاب بهترین مسیر از طریق الگوریتم دایج کسترا انجام

1 - Optimized Link State Routing Protocol ( OLSR )

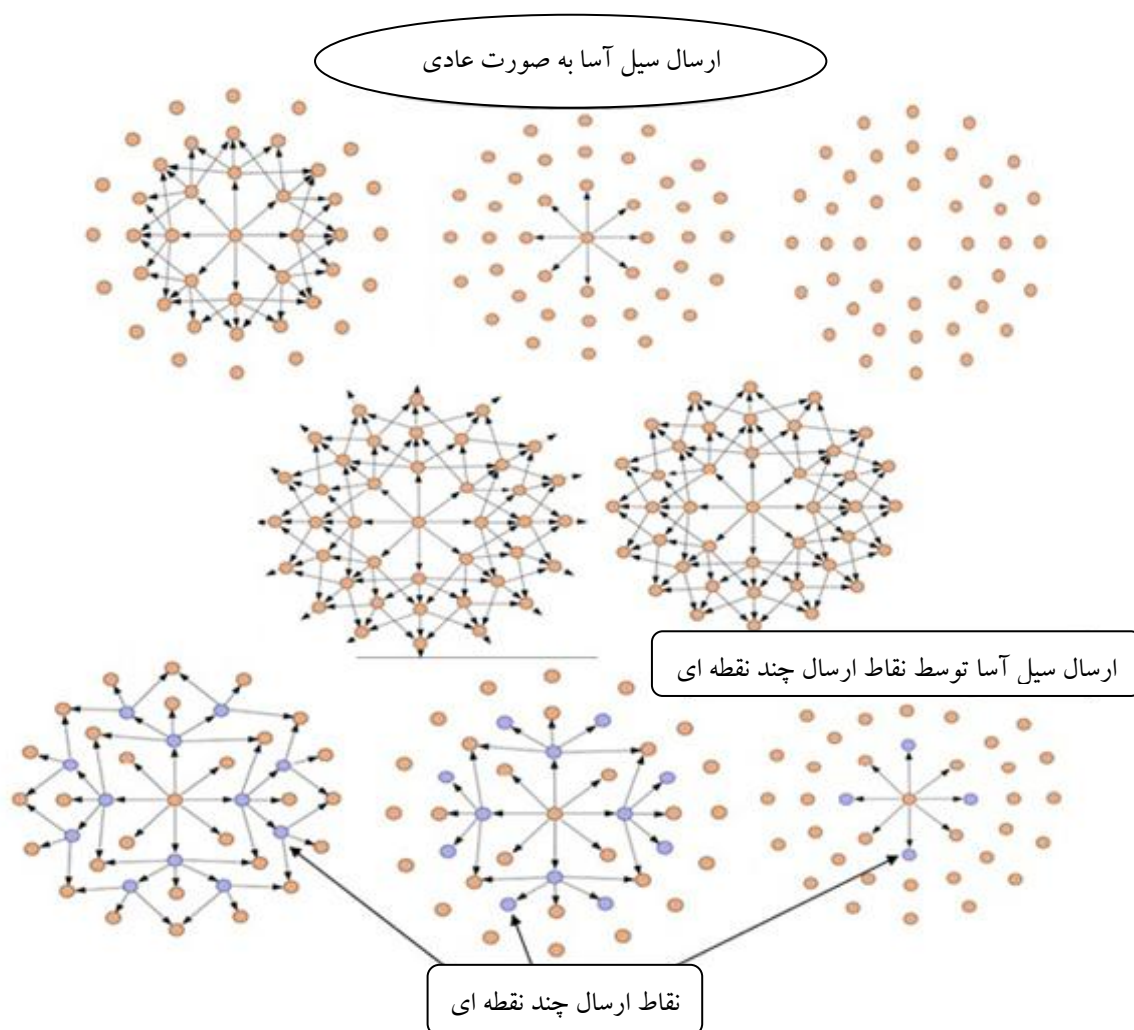
2 - Multi Point Relays ( MPR )

3 - Topology Control ( TC )

می شود . بعد از این مرحله هر نود جدول مسیریابی در اختیار دارد که بهترین مسیر به نودهای اطراف را در بر دارد. در این حالت شبکه به پایداری می رسد. با عوض شدن جای نودها عملیات بالا دوباره تکرار می گردد و جداول به روز می شوند.

تفاوت این پروتکل با مسیریابی بر مبنای حالت لینک در این است که مسیریابی بر مبنای حالت لینک برای پخش اطلاعات از روش سیل آسا استفاده می کند یعنی بسته های کنترلی را برای تمام نودهای اطراف می فرستد و این نودها هم برای همسایه های خود می فرستند و این روش باعث به وجود آمدن سربار در شبکه می شود . این پروتکل پیام ها را که لزومی ندارند دوباره فرستاده شوند را کنترل می کند. در این پروتکل تنها یک زیرمجموعه از همسایه ها (ارسال چند نقطه ای) هستند که می توانند پیام های کنترلی را دوباره ارسال نمایند. با این خاصیت ، پیام های ارسالی که به روش سیل آسا ارسال می شود ، کاهش پیدا کرده و برای کار در شبکه هایی که متراکم هستند مناسب می باشد. این روش مسیریابی نود های متحرک را پشتیبانی می کند و ارتباطات از نوع بدون اتصال می باشند .

ایده انتقال دهنده چند نقطه ای به وسیله کم کردن ارسال های مجدد در همان ناحیه خود ، پیام های سیل آسا را به حداقل رسانده است . هر نود در شبکه انتخاب می کند نودهای همسایه خود را که در فاصله یک گام از آن قرار دارد (نودهای متقارن) . که ممکن است پیام هایی را دوباره برای آن ارسال کند که این مجموعه نودها را نقاط ارسال یا انتقال دهنده چند نقطه ای گویند . همسایه هایی از نود  $N$  که در زیر مجموعه نقاط ارسال چند نقطه ای نیستند ، تنها پیام های فراگیر را دریافت و پردازش می کنند ولی این نودها اقدام به ارسال مجدد نمی کنند . تنها نودهای ارسال چند نقطه ای ، بسته های فراگیر را ارسال می کنند . نودهای انتقال دهنده چند نقطه ای هر نودی از میان همسایه هایی که متقارن با یک گام از آن قرار دارند، انتخاب می شوند . این مجموعه انتخاب ، پوشش می دهند نودهایی را که هم در فضای رادیویی قرار گرفته باشند و هم در فاصله متقارن دو گام قرار داشته باشند. هر نود، جدول مسیریابی به مقصدهایی که به واسطه نودهای ارسال چند نقطه ای شناسایی شده اند ، ذخیره می کند . به صورت دوره ای هر نود لیست نودهای ارسال چند نقطه ای خود را پخش می کند ( در عوض ارسال لیست همه همسایه های خود ، فقط لیست نقاط ارسال چند نقطه ای خود را ارسال می کند) . به محض دریافت اطلاعات نقاط ارسال چند نقطه ای ، هر نود اطلاعات مسیریابی به مقصدی که می شناسد را به روز می کند . در شکل های زیر ابتدا شبکه ای را دنبال می کنید که در آن بسته ها به صورت سیل آسا برای همه ارسال می شود ، ولی با این پروتکل این روند کاهش پیدا کرده و ارسال بسته ها به دلیل نودهای ارسال چند نقطه ای کاهش پیدا می کند و این باعث کاهش سربار در شبکه می شود .



شکل ۴-۲۲ پیدا کردن گره های ارسال چند نقطه ای در پروتکل مسیریابی حالت پیوند بهینه

#### ۴-۶-۱ انواع پیام ها

#### ۴-۶-۱-۱ پیام سلام<sup>۱</sup>

وظیفه پیام سلام که به صورت دوره ای توسط نود ها ارسال می شود عبارتند از :

۱ - حس لینک ( وجود داشتن ارتباط )

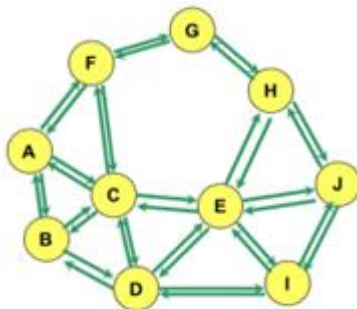
۲ - کشف همسایه ها

۳ - علامت گذاری گره های انتقال دهنده چند نقطه ای

هر نود برای تعیین مجموعه نقاط ارسال چند نقطه ای از پیام سلام استفاده می کند. هر نودی به طور دوره ای پیام سلام را برای همسایه های خود پخش می کند که به این طریق همسایه های خود را کشف می کند (لینکهای دو طرفه). پیام سلام به هر نود اجازه می دهد که توپولوژی شبکه را تا دو گام فراگیرد و نودهای ارسال چند نقطه ای



را علامت گذاری نماید . یک نود باید کمترین ارسال ها بین خودش با نودها را برای تعیین کردن نقطه ارسال چند نقطه ای داشته باشد و اطلاعات کافی برای مسیریابی فعال را تهیه نماید . با استفاده از اطلاعات دریافت شده توسط پیام سلام، نودها می توانند همسایگان دوم خود و مجموعه نقاط ارسال چند نقطه ای بهینه را تعیین کنند . شماره ترتیب با مجموعه نقاط ارسال چند نقطه ای مرتبط است . شماره ترتیب هر زمانی که مجموعه جدید محاسبه می شود افزایش پیدا می کند . پیام سلام همچنین همسایه هایی که جزء مجموعه ارسال چند نقطه ای هستند را نشان می دهد . مجموعه ارسال چند نقطه ای زمانی که یک تغییر در اولین همسایه یا دومین همسایه رخ دهد دوباره محاسبه می شود

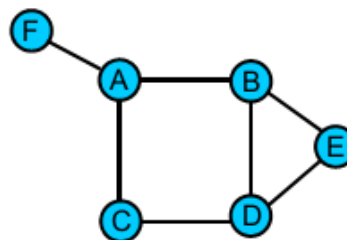


شکل ۴-۲۳ کشف همسایه - تا دو گام همسایه ها را شناسایی می کند

#### ۴-۶-۱-۱-۱ الگوریتم انتخاب نقاط ارسال چند نقطه ای

در این پروتکل هر نود با فرستادن پیام سلام تا دو گام می تواند همسایه های خود را شناسایی نماید . محتوای هر پیام سلام، لیست همسایه ها می باشد . در شکل زیر یک بخشی از ارسال و دریافت پیام سلام برای پیدا کردن نود ارسال چند نقطه ای مشخص می باشد . ابتدا نود A یک پیام سلام خالی برای همسایه های خود ارسال می نماید . سپس همسایه های A یعنی B, F, C پیام سلامی به محتوای همسایه بودن با A برای نود A ارسال می کنند . نود A با کشف همسایه های خود، یک پیام سلامی با محتوای همسایه های خود ارسال می نماید . در این صورت نود F متوجه می شود تا دو گام با نود های B, C همسایه می باشد . در این وضعیت همه نودها، همسایه های خود تا دو گام را شناسایی می کنند و قسمتی از توپولوژی شبکه تا دو گام را مشاهده می نمایند .

- A sends empty HELLO\_A{ }.
- A receives HELLO\_B{A}.
- A receives HELLO\_F{A}.
- A receives HELLO\_C{A}.
- A sends HELLO\_A{B,C,F}.
- F learns 2 hop neighbors: B,C.



شکل ۴-۲۴ پیدا کردن نود ارسال چند نقطه ای - شناسایی همسایه ها تا دو گام

بارد و بدل کردن پیام های سلام ، نود A همسایه های خود تا دو گام را شناسایی می کند و مختصری از توپولوژی دو گام را فرا می گیرد . حال نود A باید انتخاب کند ، حداقل تعدادی از همسایه های مستقیم خود را که اجازه دسترسی در ناحیه ای با دو گام را داشته باشد . ( به طور واضح تر یعنی : نود A از طریق نودی که ارسال چند نقطه ای خود قرار می دهد به مقصد تا دو گام فاصله دارد ) حال ارسال چند نقطه ای نود A به صورت زیر مشخص می شود:

(۱) نود A ، نود B را انتخاب می کند .

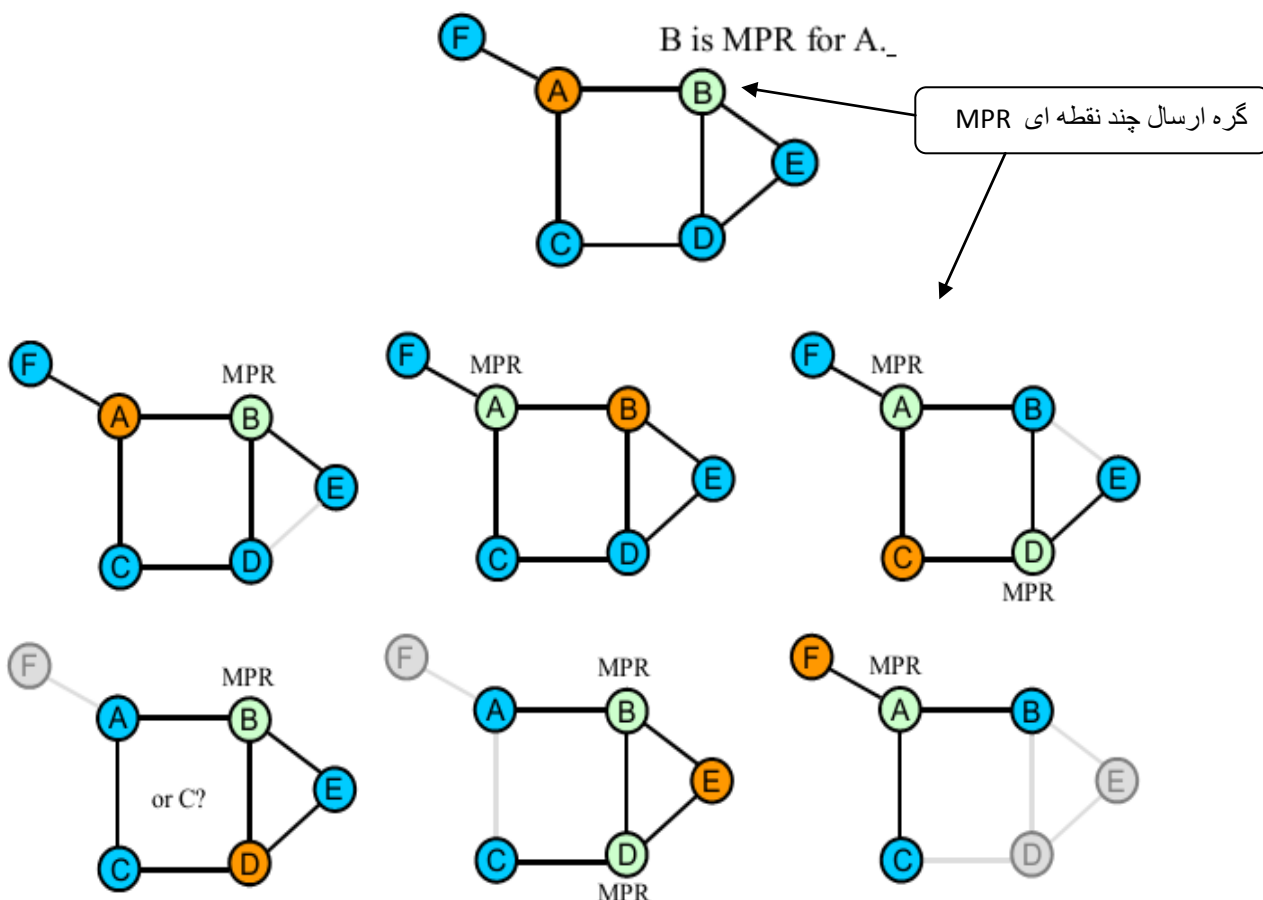
(۲) نود B ، برای ارسال چند نقطه ای نود A انتخاب می شود .

(۳) حال نود A پیام سلامی به محتوای  $\text{HELLO\_A}\{B_{\text{MPR}}, C, F\}$  ارسال می نماید . در محتوای سلام نود A

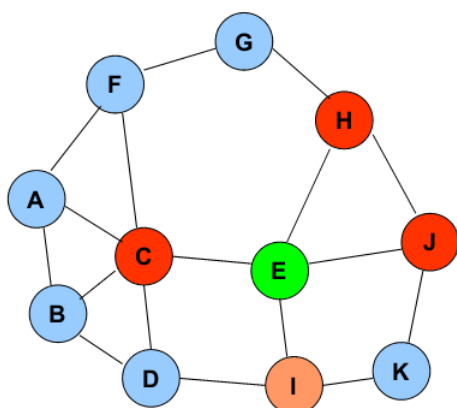
، نود B به عنوان ارسال چند نقطه ای و نودهای F, C همسایه های نود A می باشند . با ارسال این پیام ، نود B

متوجه می شود که یک ارسال چند نقطه ای برای نود A می باشد.

بقیه نودها نیز طبق شکل زیر نودهای ارسال چند نقطه ای خود را مشخص می نمایند .



شکل ۴-۲۵ انتخاب نود ارسال چند نقطه ای در پروتکل مسیریابی حالت پیوند بهینه

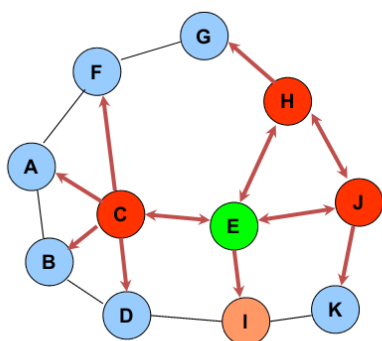


فقط نقاط ارسال چند نقطه ای می توانند بسته ها را دوباره ارسال نمایند .

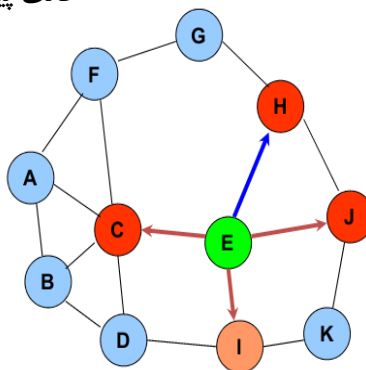
گره مرجع E  
گره با ۱ گام I  
گره ارسال چند نقطه ای C,H,J  
گره با ۲ گام K,D,B,A,F,G

شکل ۴-۲۶ ارسال مجدد پخش کردن پکت ها تنها از طریق نقاط ارسال چند نقطه ای در پروتکل مسیریابی

حالت پیوند بهینه



گره مرجع E  
گره با ۱ گام I  
گره ارسال چند نقطه ای C,H,J  
گره با ۲ گام K,D,B,A,F,G



گره مرجع E  
گره با ۱ گام I  
گره ارسال چند نقطه ای C,H,J  
گره با ۲ گام K,D,B,A,F,G

شکل ۴-۲۷ ارسال پیام به همسایه ها برای آگاه شدن از انتخاب آنها به عنوان نقاط ارسال چند نقطه ای در

پروتکل مسیریابی حالت پیوند بهینه

#### ۴-۶-۱-۲ پیام کنترل توپولوژی<sup>۱</sup>

این پیام توپولوژی شبکه را اظهار می کند . (آگاهی وضعیت لینک ها) و نودها اطلاعات توپولوژی را به وسیله پیام کنترل توپولوژی می فرستند . پیام کنترل توپولوژی به صورت دوره ای فرستاده می شود . این پیام ها در صورت تغییرات فرستاده می شوند و اگر تغییراتی صورت نگیرد ، ارسال نمی گردند . این پیام نیز لیستی از اطلاعات مربوط به همسایه ها را در خود دارد . محتوای این پیام ها به صورت زیر می باشد:

۱ - جدول انتخاب انتقال دهنده چند نقطه ای

۲ - شماره ترتیب (برای جلوگیری از استفاده مجدد اطلاعات قدیمی)

جداول مسیریابی بر مبنای جداول توپولوژی محاسبه می شوند که این جداول توپولوژی مبنی بر پیامهای کنترل توپولوژی می باشند . پیام های کنترل توپولوژی در صورت نقص لینک نیز ارسال می شوند . فقط نودهای انتقال

دهنده چند نقطه ای می توانند پیام کنترل توپولوژی را تولید کنند و همه نودها اجازه انتشار ندارند . نودها پیام کنترل توپولوژی را برای همسایه هایی که در مجموعه MS هستند تولید می کنند (MS نودهایی هستند که در مجموعه نقاط انتقال دهنده چند نقطه ای وجود دارد). تمام نودها پیام کنترل توپولوژی را دریافت می کنند اما فقط پیام کنترل توپولوژی توسط مجموعه MS پخش می شود .

#### ۴-۶-۲ جدول مسیریابی

در جداول مسیریابی ، مقصدهایی که در شبکه شناسایی شده اند نگهداری می گردد . جداول مسیریابی از طریق جداول توپولوژی و جفت های متصل شده محاسبه می گردند که این محتوای این جداول شامل موارد زیر می باشد :

۱ - آدرس مقصد

۲ - آدرس گام بعدی

۳ - فاصله مسیر

جدول مسیریابی بعد از هر تغییری در جدول همسایه یا جدول توپولوژی به روز می شود و در این پروتکل جهت شناسایی کوتاه ترین مسیر از الگوریتم دایجکسترا استفاده می گردد.

#### ۴-۶-۳ خصوصیات پروتکل OLSR

- (۱) تنها MPR پیغامهای کنترلی را دوباره می فرستد
- (۲) اندازه پیغامهای کنترلی را کاهش می دهد
- (۳) سربرار شبکه را کم می کند
- (۴) پروتکل پایدار است و از نوع فعال می باشد .
- (۵) به هیچ موجودیت مرکزی وابستگی ندارد
- (۶) تحرک و پویایی نودها را ساپورت می کند و برای شبکه های متراکم مناسب است

#### ۴-۷ جمع بندی

در این فصل با روش های مختلف تقسیم بندی پروتکل های مسیریابی ، با انواع الگوریتم های مسیریابی آشنا شدیم . هر کدام از این روشها یا الگوریتم ها برای اجرا در شبکه ها شرایط خاص خود را دارند . برای مثال روش های بر حسب تقاضا در شبکه های با پویایی بالا نرخ اتلاف<sup>۱</sup> کمتری نسبت به مشی های کنش گر دارند در

حالیکه در پویایی پایین این موضوع بالعکس است، در مورد تاخیر در روش های کنش گر چون اغلب اطلاعات لازم مسیریابی از قبل ارسال شده است مسلماً تاخیر کمتری نسبت به روش های برحسب تقاضا دارند. در زمینه سربار مسیریابی چون در روش های کنش گر ارسال های دوره ای داریم، سربار بالاتری هم مشاهده می شود که البته ثابت است و اگر ملاک ارزیابی را تراکم گره های شبکه در نظر بگیریم می توان گفت که با افزایش تراکم شبکه پروتکل های بر حسب تقاضا کارایی تاخیر را بهتر نگه می دارند، چون ارسال های دوره ای ندارند. در مجموع می توان گفت که مشی های بر حسب تقاضا روش های بهتری به نظر می رسند.

در پروتکل DSR علامت این که پروتکلی واکنشی است به خاطر تعدد پیام هایی نظی RERR, RREP RREQ همچنین اطلاعاتی که گره ها به این پیام ها اضافه می کند حجم تبادل اطلاعات کنترلی در شبکه زیاد است. از طرفی AODV اساساً پروتکلی است برگرفته از DSDV که خود بر مبنای الگوریتم بردار فاصله عمل می کند. حال آن که DSR بر اساس موقعیت بهند بنا نهاده شده است لذا می توان نتیجه گرفت حجم اطلاعات کنترلی در شبکه هنگام استفاده از AODV کمتر از DSR است. البته اگر بررسی را با جزئیات بیشتری انجام دهیم مشاهده می کنیم که طول قالب در بسته ی کنترلی AODV که مابین گره های واسط رد و بدل می شوند نفی از DSR کمتر است و این خود بهی کمتر بودن سرباره های کنترلی در AODV نسبت به DSR. می دانیم هر چه اطلاعات گره ها راجع به موقعیت کلی شبکه بیشتر باشد نظیر به تبادل اطلاعات کنترلی کمتر پیش می آید پس مجهز نمودن گره ها به ادواتی چون GPS و استفاده از پروتکل های مبتنی بر موقعیت جغرافیایی می تواند سرباره های کنترلی را کاهش دهد. بعلاوه می توان با به کار گیری پردازنده های قوی تر و تجهیزات چون آنتن های هوشمند این سرباره ها را به حداقل رساند. در فصل بعد با ایجاد کرن محیط شبکه اقتضائی در نرم افزار شبیه ساز و پیاده سازی پروتکل های مسیریابی AODV, DSR, OLSR در آن، نتایج شبیه سازی را بدست می آوریم و بررسی خواهیم نمود.

## فصل پنجم

### شبیه سازی

## ۱-۵ مقدمه

امروزه با رشد چشمگیر شبکه های کامپیوتری روشهایی که بتوان توسط آنها رفتار شبکه ها را آنالیز و بررسی کرد از اهمیت فراوانی برخوردارند. همچنین طراحان شبکه برای آزمایش ایده های نوین خود نیازمند ابزارهایی جهت شبیه سازی رفتار شبکه ها هستند. نرم افزارهای شبیه ساز ابزار مناسبی برای شبیه سازی شبکه ها هستند. بخصوص برای شبکه های امروزی که دارای ساختار با پیچیدگی بالا بوده و استفاده از روشهای آنالیز ریاضی در بررسی رفتار آنها عملاً به صورت دقیق امکان پذیر نیست. از جمله شبیه سازهای شبکه می توان به ++OMNET, U-Net, Ns-2, Maisie, NetSim, INSANSE, REAL اشاره کرد. همچنین نرم افزارهای شبیه سازی تجاری متعددی نیز وجود دارند که از جمله مهمترین آنها می توان به شبیه سازهای OPNET, COMNET, BONEs اشاره کرد. در اینجا به طور مختصر به هر یک از این شبیه سازها و کاربرد آنها اشاره می کنیم: شبیه ساز REAL برای بررسی رفتار پویا و متغیر روشهای مختلف کنترل ازدحام و کنترل جریان در شبکه های داده با سوئیچینگ بسته ای به کار می رود. در این نرم افزار توپولوژی شبکه، پروتکل های مختلف و همچنین پارامترهای کنترلی به صورت یک سناریو تعریف می شوند. همچنین بیش از ۳۰ ماژول مختلف در این نرم افزار آماده شده است که می توان با استفاده از آنها رفتار پروتکل های مختلف کنترل جریان و ازدحام را به صورت دقیق شبیه سازی و تقلید کرد. شبیه ساز INSANCE برای بررسی رفتار الگوریتم های مختلف در زمینه IP روی ATM طراحی شده است. شبیه ساز NetSim به منظور مدل کردن دقیق استاندارد اترنت و بررسی معضلات موجود در آن به کار می رود. شبیه ساز Maisie مبتنی بر زبان برنامه نویسی C بوده و برای شبیه سازیهای سلسله مراتبی مناسب است.

## ۲-۵ آشنایی با مفاهیم اولیه نرم افزار شبیه سازی (OPNET<sup>1</sup>)

شبیه سازهای شبکه را از دیدگاههای مختلف می توان تقسیم بندی کرد. یکی از این دیدگاهها برای تقسیم بندی شبیه سازهای شبکه روشی است که برای شبیه سازی به کار می برند. به طوریکه در حالت کلی شبیه سازی به دو روش متفاوت صورت می گیرد. روش اول شبیه سازی به کمک آنالیز دقیق رویدادها و روش دوم شبیه سازی رویدادهای گسسته است. در روش اول برای شبیه سازی از مدل های ریاضی برای حصول نتایج استفاده می شود و شبکه با مجموعه ای از معادلات ریاضی مدل می شود. عیب عمده این روش شبیه سازی در ساده کردن بیش از حد شبکه در این مدلها و عدم توانایی در شبیه سازی رفتار پویای شبکه ها است. اما در روش دوم شبیه

سازی ( در سطح پایین در سطح بسته های موجود در شبکه) انجام شده و از این رو نتایج از دقت بالایی برخوردارند. در این روش نتایج با شبیه سازی رویدادهای گسسته به دست می آیند. اما بر خلاف روش اول که شبیه سازی با سرعت بالایی انجام می شود، در این شبیه سازها نتایج با سرعت کمی حاصل خواهند شد اما راه حل مناسب، استفاده از ترکیب این دو روش در شبیه سازی با هدف داشتن عملکرد مورد قبول و حفظ دقت مورد نیاز در موارد بحرانی است. این شبیه سازها را اصطلاحاً شبیه سازهای مرکب یا دو رگه گویند. از مهمترین این شبیه سازها می توان به OPNET و NS-2 اشاره کرد. شبیه ساز NS-2 نسخه دوم شبیه ساز شبکه است که توسط VINT گسترش داده شده است. NS-2 یک شبیه ساز شبکه مبتنی بر رویداد است که به وفور توسط مهندسين شبکه مورد استفاده قرار می گیرد. در این شبیه ساز مدل های مختلفی از اغلب پروتکل های اینترنت را در خود دارد و همچنین به دلیل باز بودن منبع آن دارای سطوح مختلف پیکربندی بوده و همچنین قابلیت ایجاد پروتکلها و کاربردهای متداول را دارا می باشد.

OPNET همانطور که از نام آن مشخص است، نرم افزاری است که دستیابی به عملکرد بهینه را ممکن می سازد. قابلیت های این نرم افزار در شبیه سازی جنبه های مختلف شبکه، از لایه کاربرد گرفته تا لایه های فیزیکی، حیرت انگیز است. این نرم افزار به طراحان و محققان اجازه می دهد عملکرد پروتکل ها و تجهیزات را با دقت قابل قبولی از طریق شبیه سازی پیش بینی کنند. قابلیت های این نرم افزار واقعاً پایان ناپذیر است. کاربردهای مهم OPNET عبارتند از: آنالیز شبکه های فعلی از طریق شبیه سازی، طراحی بهینه شبکه، شبیه سازی عملکرد پروتکل های جدید که در محیط های تحقیقاتی به وجود آمده اند، انعطاف در مدل سازی، سهولت در مدل سازی، اجرای سریع مدل ها، قابلیت مصور سازی و قابلیت اجرای مجدد و تکراری شبیه سازی و ...

## ۳-۵ پارامترهای ارزیابی

### ۳-۵-۱ میزان تاخیر<sup>۱</sup>

مدت زمانی که طول می کشد تا اطلاعات از مبدا به مقصد منتقل گردد که شامل ۴ منبع می باشد.

(۱) تاخیر پردازش: که شامل چک کردن پیریتی و مشخص کردن لینک خروجی برای هر بسته می باشد.

(۲) تاخیر صف: که در صورت وجود ازدحام ایجاد می گردد.

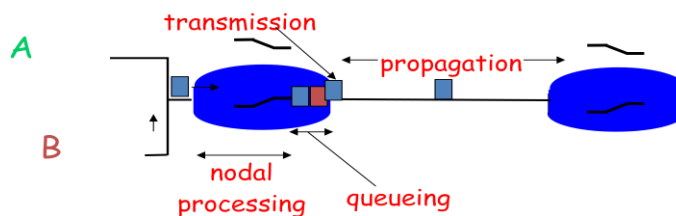
(۳) تاخیر انتقال: مدت زمانی است که طول می کشد بیت ها از اینترفیس خارج و روی لینک خروجی قرار

داده شود



۴) تاخیر انتشار: که زمانی است که طول می کشد از نقطه ای به نقطه دیگر برسد که بستگی به سرعت طی کردن و طول فیزیکی مسیر دارد.

تاخیری که در اینجا محاسبه می شود، تاخیر انتها به انتها می باشد که شامل هر ۴ تاخیر ذکر شده می باشد.



شکل ۵-۱ نمایش دهنده تاخیر انتها به انتها

### ۵-۳-۲ توان<sup>۱</sup>

نرخ کلی اطلاعات صحیحی می باشد که گیرنده از فرستنده دریافت می کند.

### ۵-۳-۳ میزان سربار<sup>۲</sup>

در اثر انتقال اطلاعات در طول مسیر مقداری از این اطلاعات در اثر ازدحام گم می گردد که این مقدار را سربار شبکه گویند.

### ۵-۳-۴ بار شبکه<sup>۳</sup>

نشان دهنده کل ترافیک شبکه بر مبنای بیت بر ثانیه می باشد.

## ۵-۴ فرآیند شبیه سازی

در فصل های گذشته با محیط شبکه های اقتضائی و خصوصیات و ساختار این شبکه ها و همچنین پروتکل های متداول مسیریابی در این شبکه ها آشنا شدیم. در این قسمت با استفاده از محیط نرم افزار شبیه ساز OPNET 14.5 قصد داریم یک شبکه اقتضائی متحرک را پیاده سازی نماییم و سپس پروتکل های مسیریابی AODV, DSR, OLSR را برای مسیریابی بین نود های شبکه، شبیه سازی نماییم.

هدف از شبیه سازی این پروتکل های مسیریابی، مقایسه میزان تاخیر، میزان سربار شبکه، بار شبکه و توان شبکه در چند حالت مختلف می باشد، تا بدین منظور، عملکرد این پروتکل ها مورد بررسی قرار گیرد.

ابتدا نرم افزار را اجرا نموده و طبق شکل های زیر محیط شبیه سازی را پیاده سازی می نماییم. فضای محیط در نظر گرفته شده ۱۰۰۰ \* ۱۰۰۰ مترمربع در یک شبکه پردیس و با ساختار شبکه های اقتضائی متحرک می باشد. در

1 - Throughput  
2 - Buffer Overflow  
3 - Network Load

اینجا ۴ محیط تعریف شده که هر محیط برای هر سه پروتکل AODV, DSR, OLSR ایجاد شده که در مجموع این پروژه دارای ۱۲ سناریو می باشد، که هر کدام به شرح زیر پیاده سازی شده است.

(۱) ایجاد ۲۰ نود متحرک موبایل با سرعت (۲.۷۷m/s) و  $10\text{ km/h}$  و یک سرور ثابت و نرخ ارسال داده

11Mbps و آدرس دهی IPv4 و استفاده از پروتکل FTP می باشد. همچنین نودها به صورت برداری و متحرک در حال حرکت می باشند.

(۲) با همان مشخصات محیط اول، با این تفاوت که ۴ حالت حرکت جدید برای ۴ نود تعریف شده که در فواصل زمانی مشخص در یک مسیر مشخص از قبل تعریف شده در حال حرکت می باشند. این محیط برای این منظور تعریف شده که پروتکل های مسیریابی نام برده در مواجهه با تغییرات توپولوژی عملکردشان چگونه است.

(۳) در این محیط ۵ نود متحرک حذف شده و با همان مشخصات قبلی با ۱۵ نود، عملکرد پروتکل ها بررسی می شود.

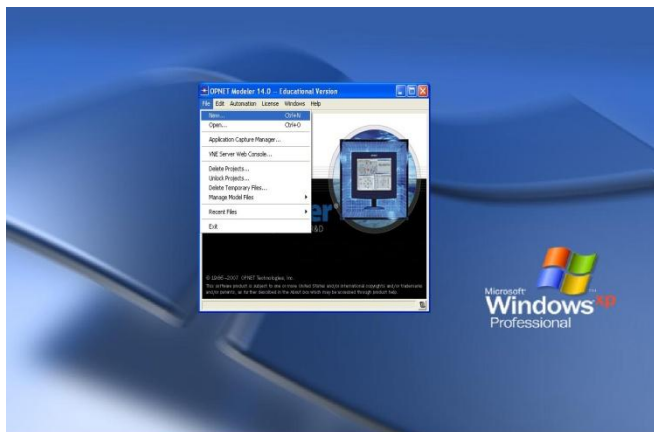
(۴) در اینجا محیط دوم ایجاد شده، با این تفاوت که سرعت حرکت نودها دوبرابر شده و  $20\text{ km/h}$  و  $(5.55\text{ m/s})$  می باشد.

پس از ایجاد کردن ۱۲ سناریو، باید شبیه سازی را اجرا کنیم. برای دیدن نتایج ما در اینجا شبیه سازی را در مدت ۵ دقیقه اجرا نمودیم و نتایج شبیه سازی را بدست آوردیم که در ادامه آنها را بررسی خواهیم نمود

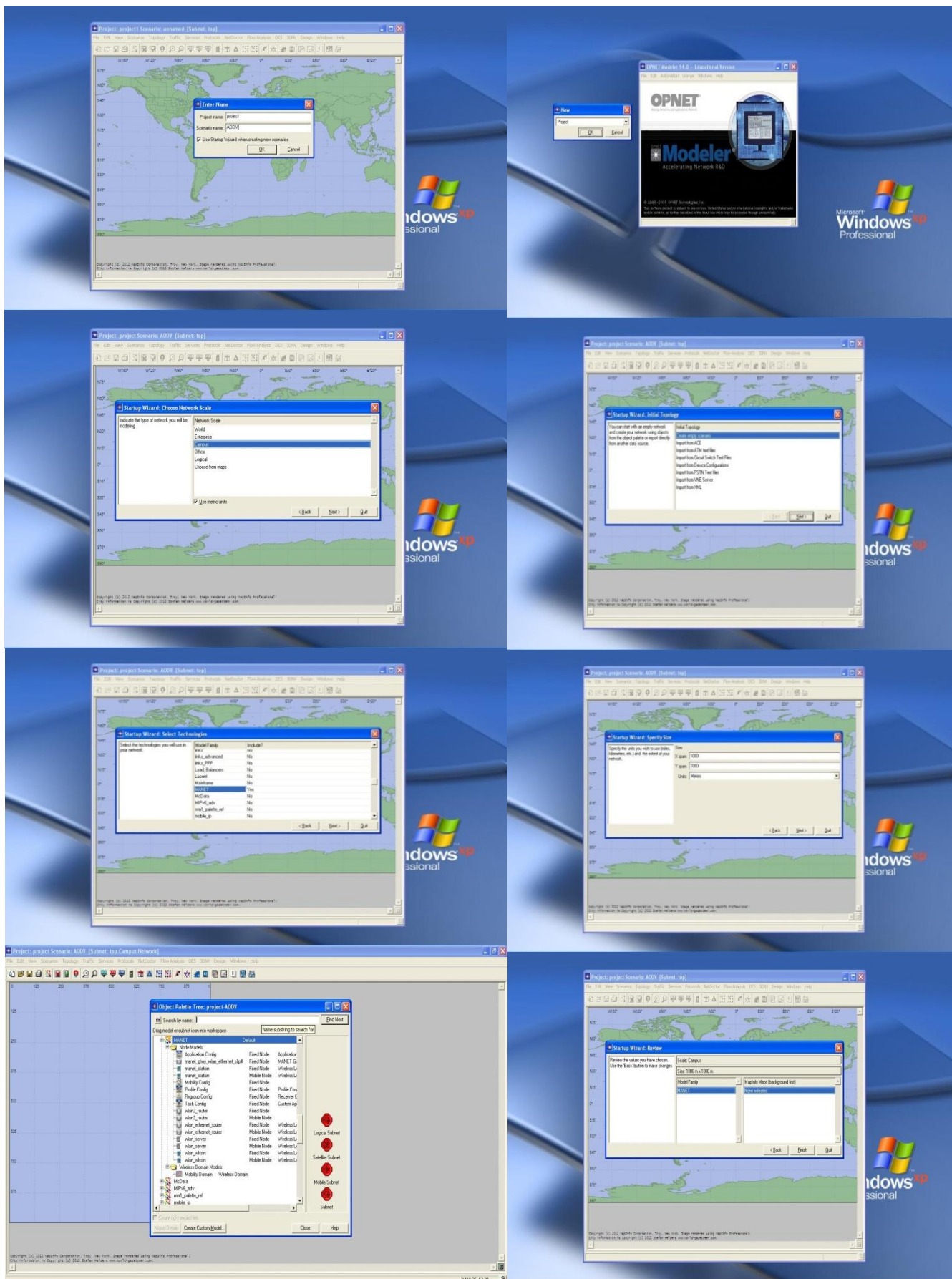
## ۵-۵ اجرای نرم افزار OPNET و پیاده سازی شبیه سازی

در شکل های زیر اجرای نرم افزار و ایجاد یک محیط شبکه MANET به همراه برخی تنظیمات آن را مشاهده می نمایید. همچنین در تصویر آخر، قسمت تجهیزات شبکه (object palette) می باشد که از این قسمت برای وارد کردن تجهیزات و ادوات شبکه استفاده می شود. در نرم افزار شبیه سازی، ۱۲ سناریو با سه پروتکل

مسیریابی AODV, DSR, OLSR تعریف شده است.



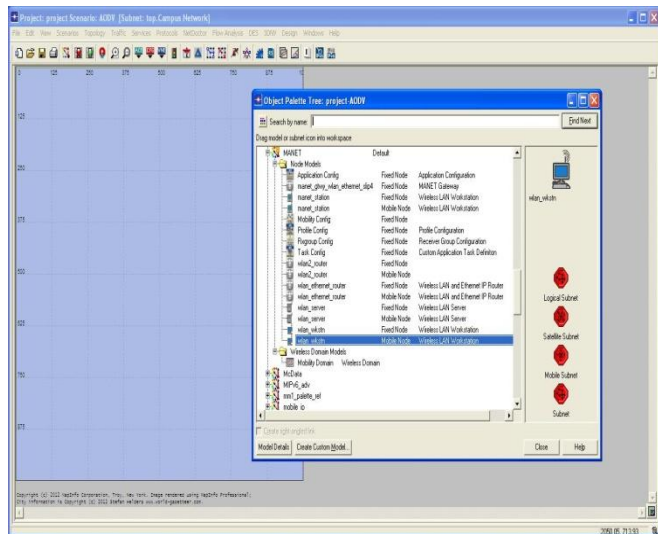
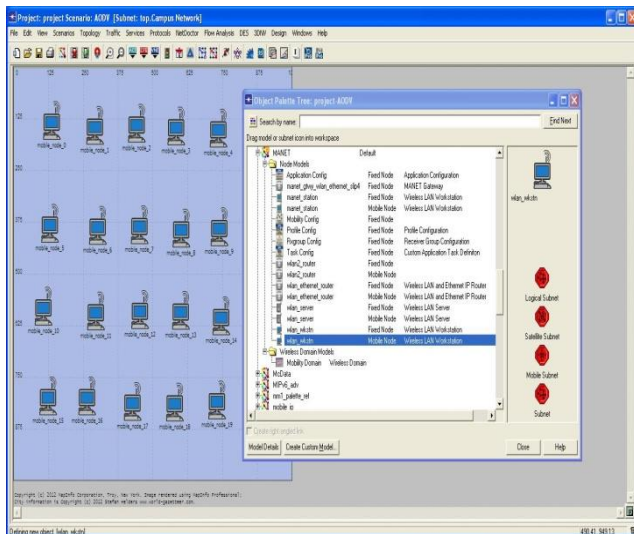
مقایسه پروتکل های مسیریابی AODV, DSR, OLSR در شبکه های اقتضائی متحرک با نرم افزار شبیه سازی OPNET



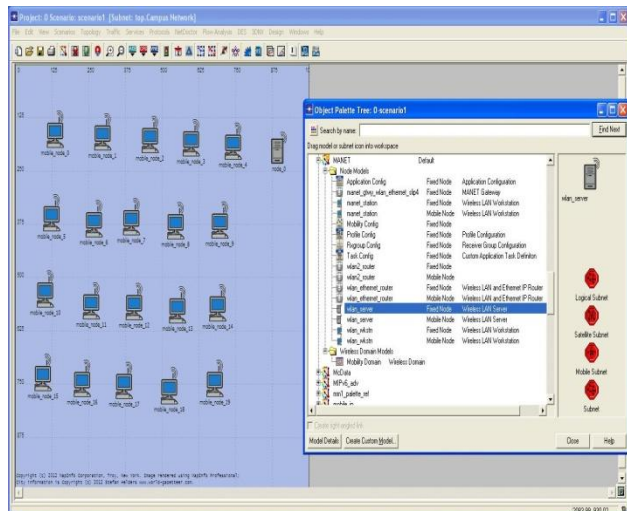
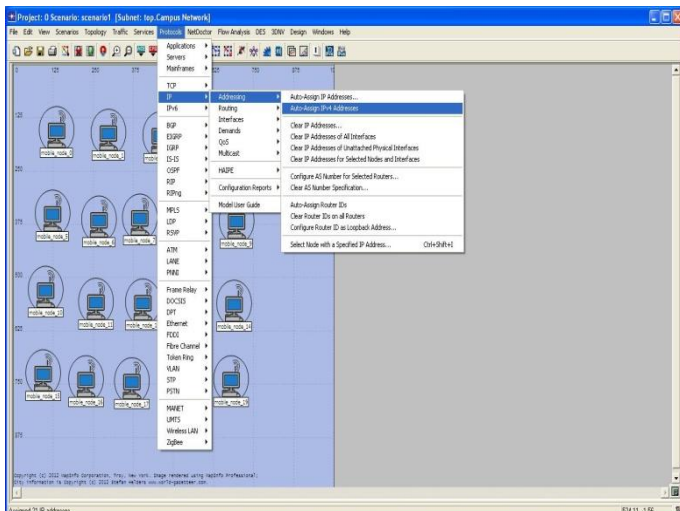
شکل ۲-۵ اجرای نرم افزار ، ایجاد محیط شبکه و قسمت تجهیزات شبکه



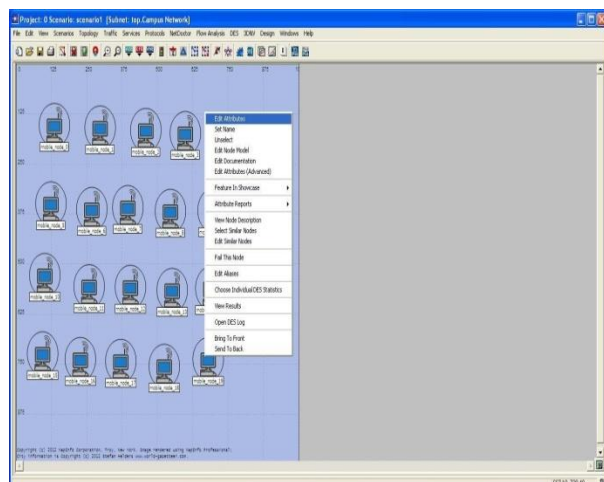
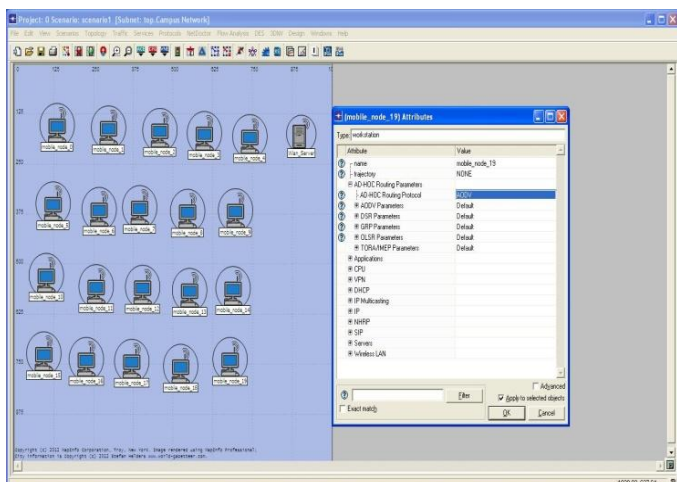
## مقایسه پروتکل های مسیریابی AODV, DSR, OLSR در شبکه های اقتضائی متحرک با نرم افزار شبیه سازی OPNET



شکل ۵-۳ قسمت تجهیزات شبکه و وارد کردن ۲۰ نود متحرک

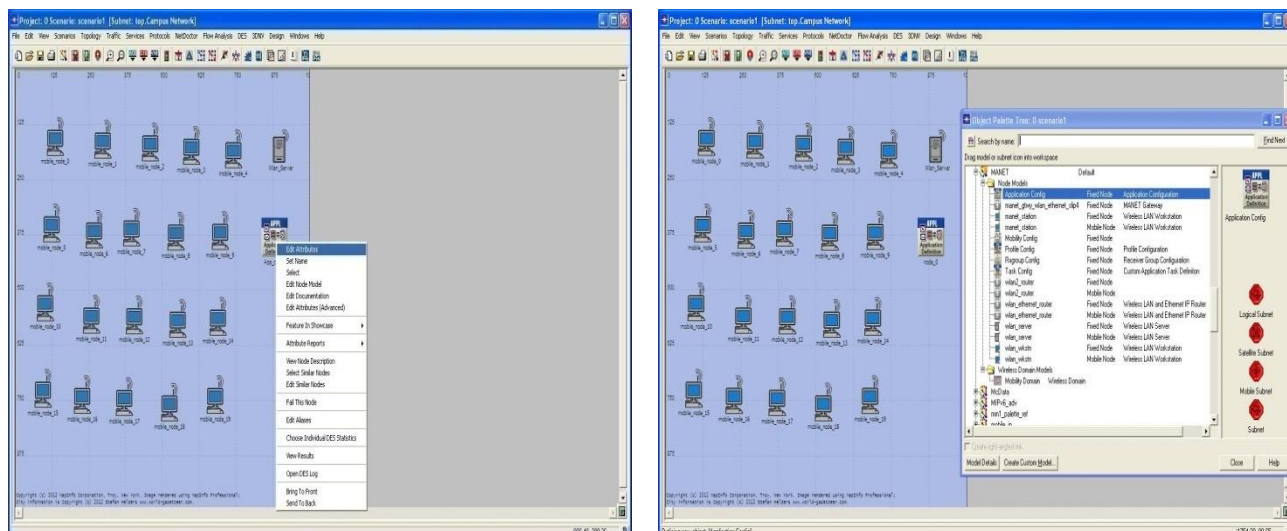


شکل ۵-۴ آوردن یک سرور ثابت و آدرس دهی IPv4

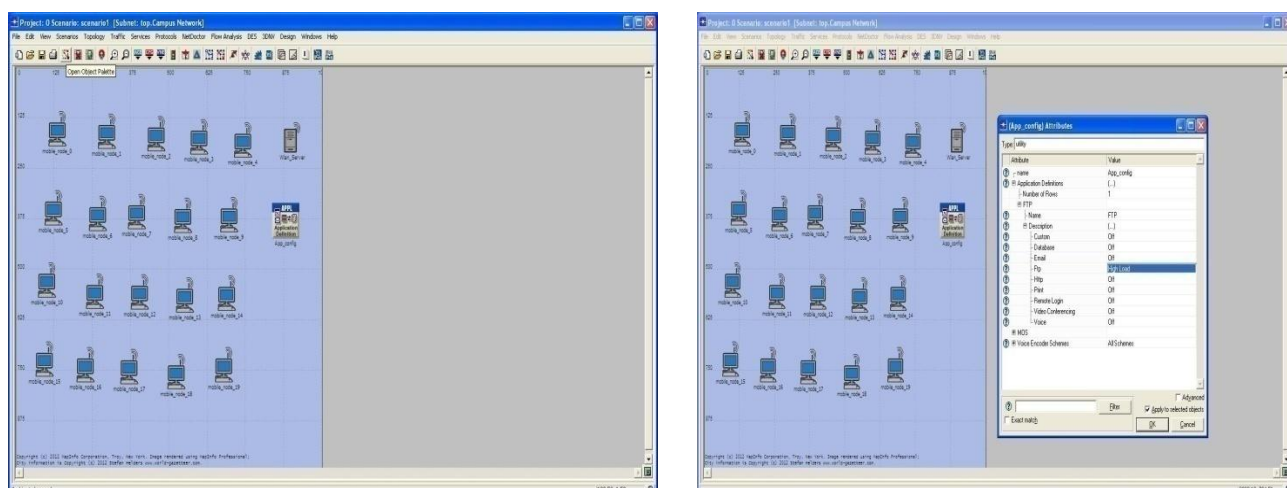


شکل ۵-۵ انتخاب نودها و ایجاد پروتکل AODV

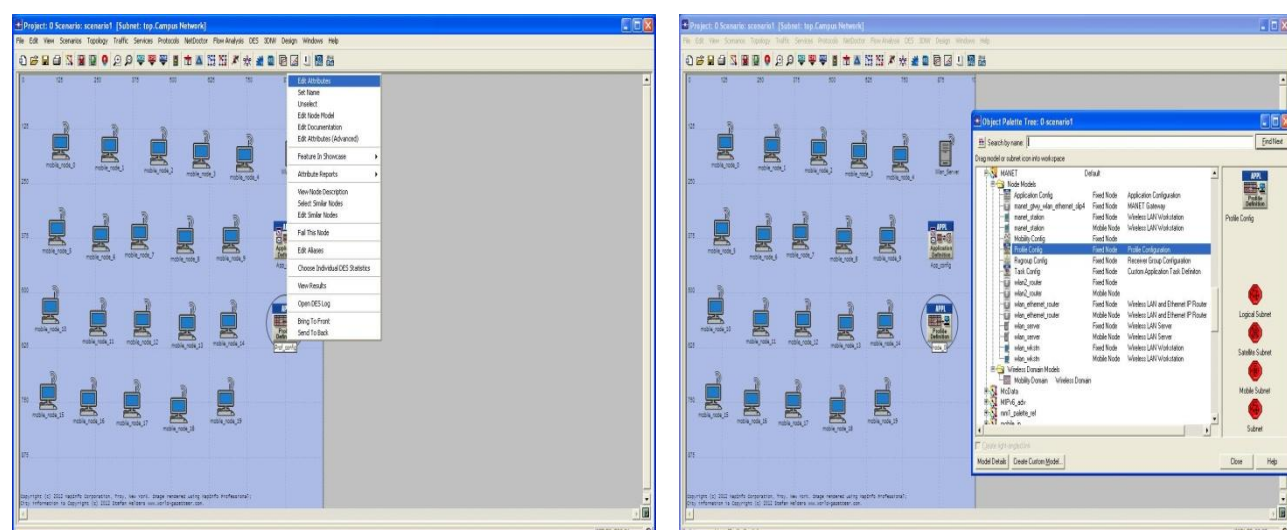
## مقایسه پروتکل های مسیریابی AODV, DSR, OLSR در شبکه های اقتضائی متحرک با نرم افزار شبیه سازی OPNET



شکل ۵-۶ انتخاب Application \_ config



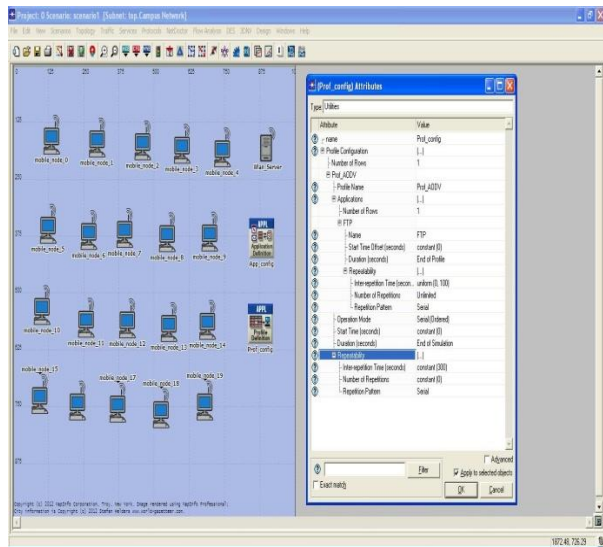
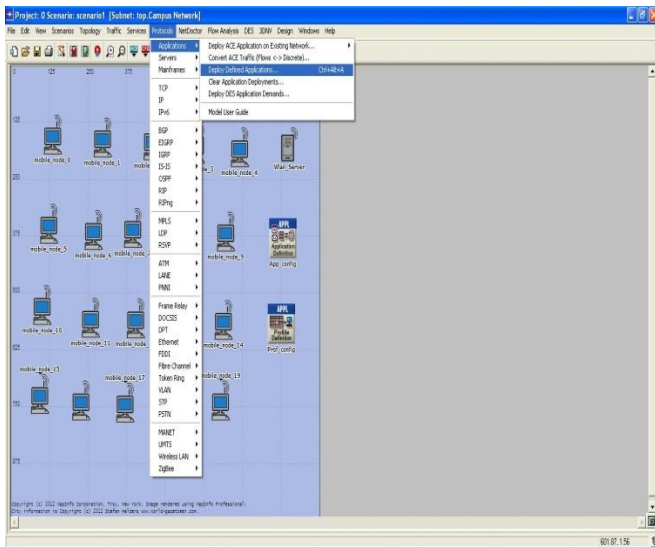
شکل ۵-۷ انتخاب پروتکل FTP



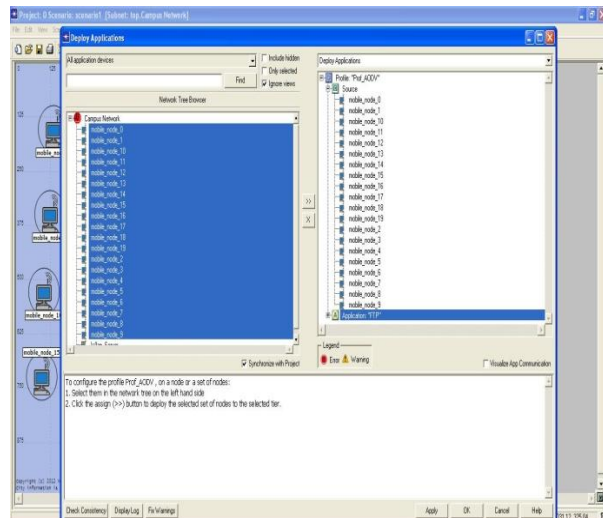
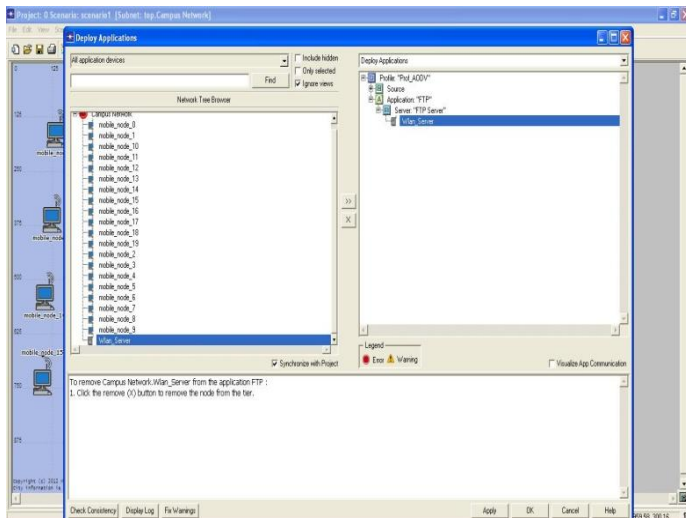
شکل ۵-۸ انتخاب Profile\_Config



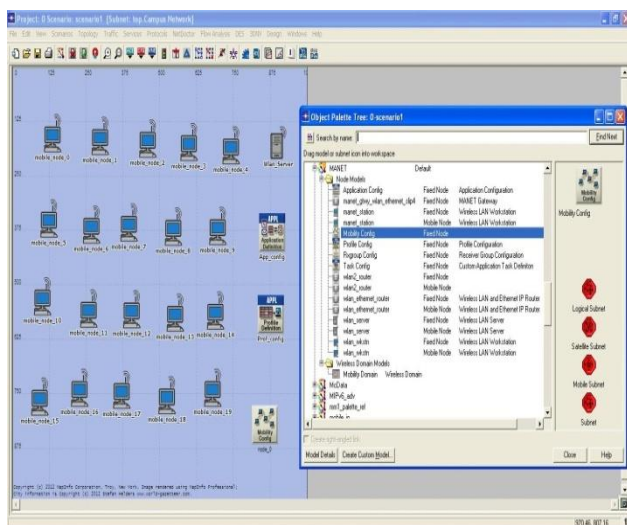
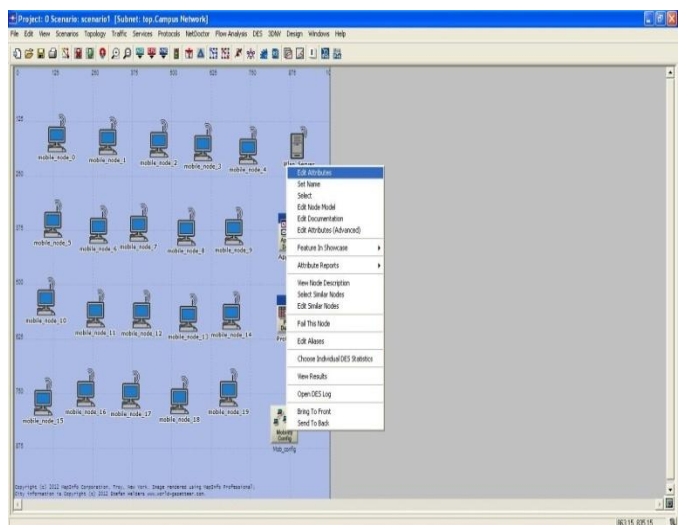
## مقایسه پروتکل های مسیریابی AODV, DSR, OLSR در شبکه های اقتضائی متحرک با نرم افزار شبیه سازی OPNET



شکل ۹-۵ تنظیمات Profile\_Config و آوردن قسمت تعریف تجهیزات

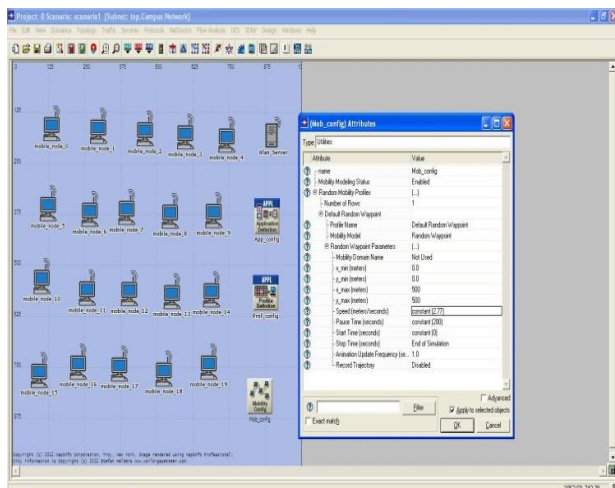
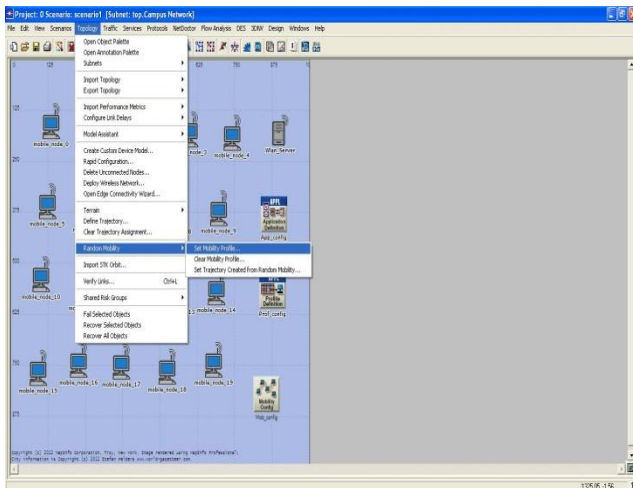


شکل ۱۰-۵ تعریف تجهیزات (نودهای متحرک و سرور ثابت) در قسمت مربوطه

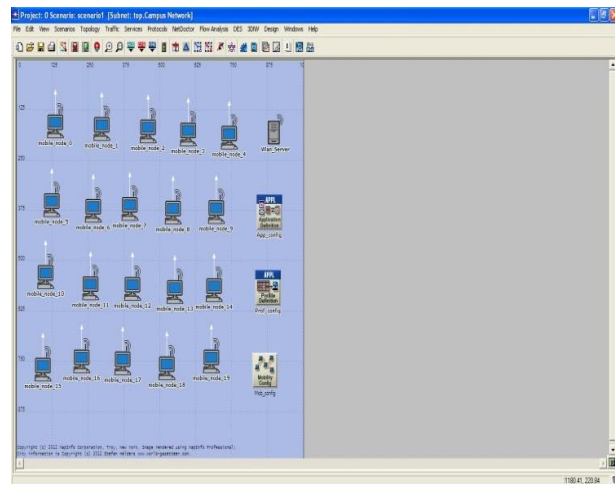
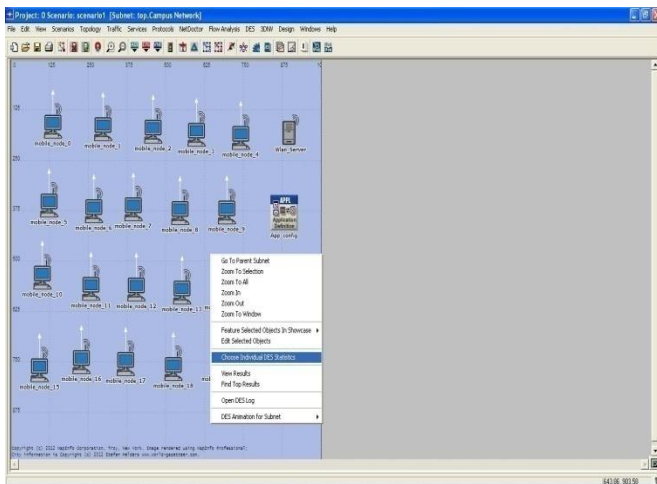


شکل ۱۱-۵ انتخاب Mobility\_Config

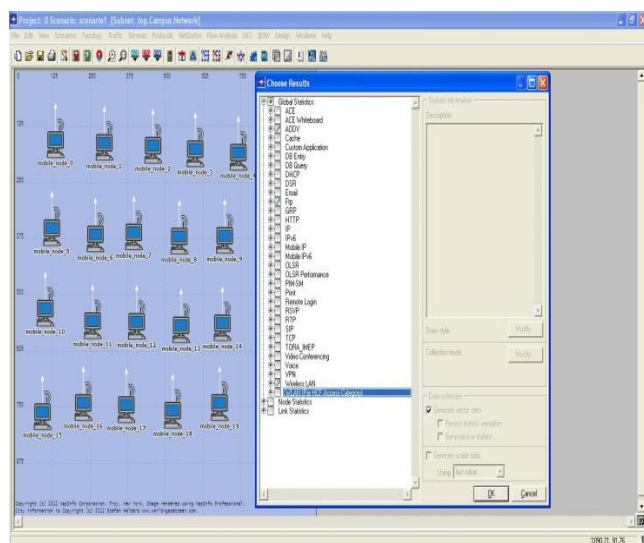
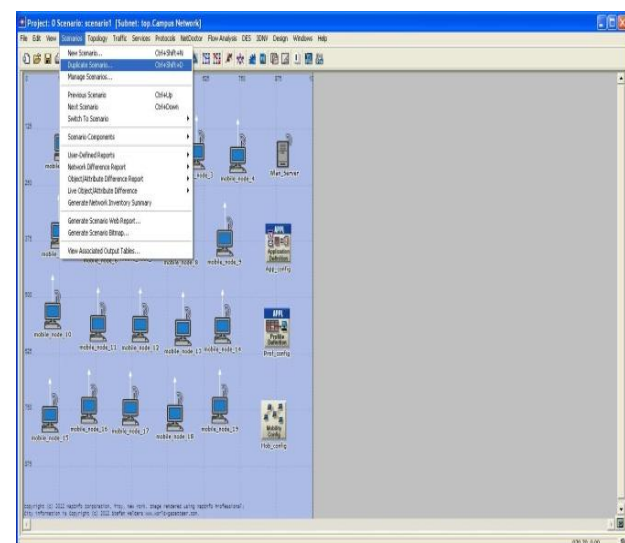
## مقایسه پروتکل های مسیریابی AODV, DSR, OLSR در شبکه های اقتضائی متحرک با نرم افزار شبیه سازی OPNET



شکل ۵-۱۲ تنظیمات Mobility\_Config و اعمال تنظیمات آن در شبکه

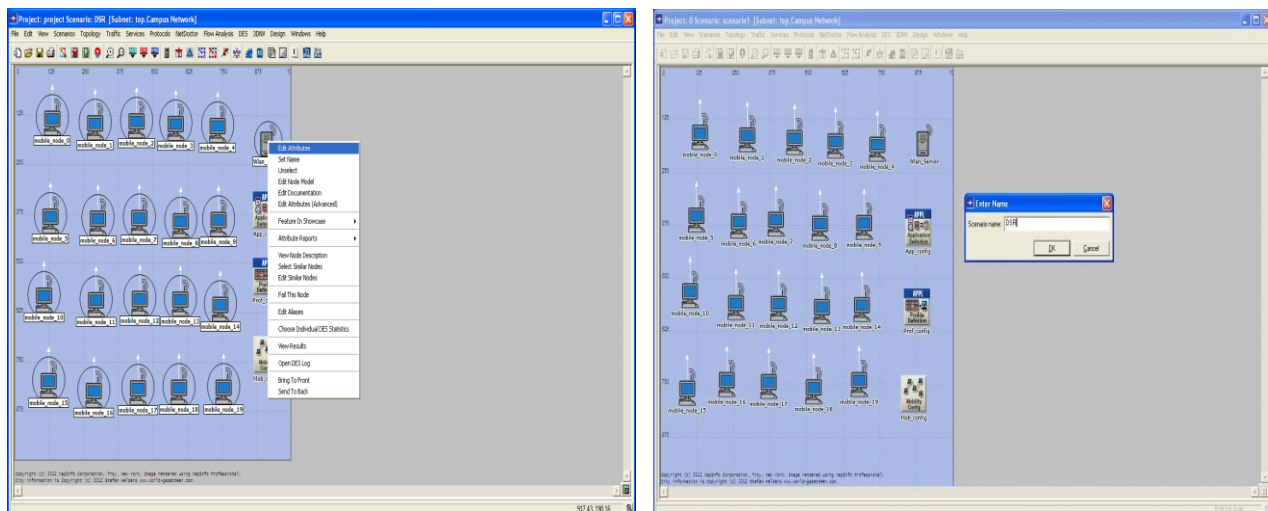


شکل ۵-۱۳ مشاهده جهت حرکت نودها و انتخاب قسمت انتخاب پروتکل ها برای مشاهده نتایج بعد از شبیه سازی

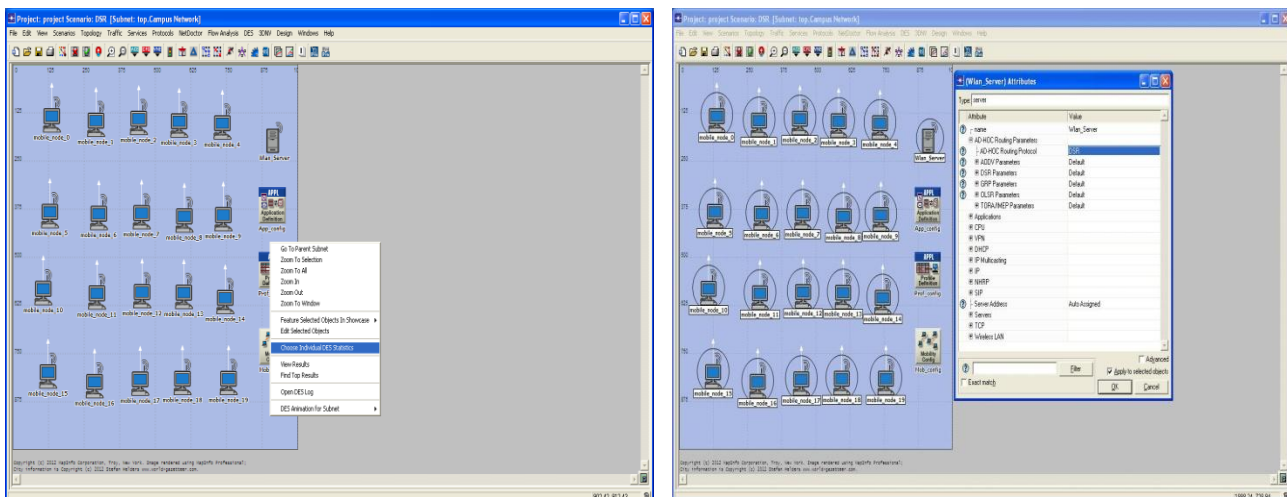


شکل ۵-۱۴ انتخاب پروتکل ها برای دیدن نتایج بعد از شبیه سازی و انتخاب سناریوی بعدی

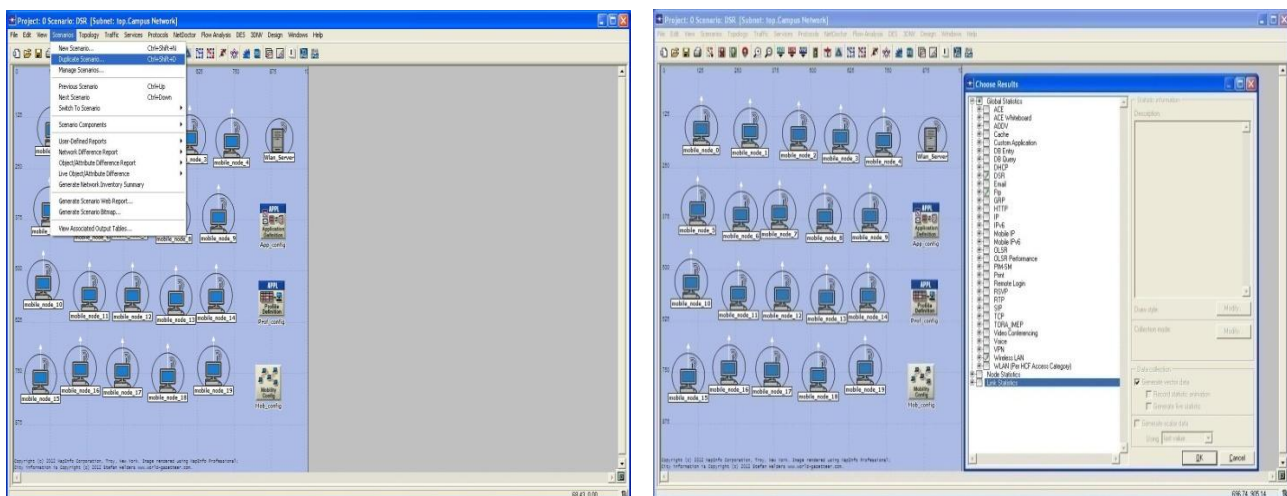
## مقایسه پروتکل های مسیریابی AODV, DSR, OLSR در شبکه های اقتضائی متحرک با نرم افزار شبیه سازی OPNET



شکل ۵-۱۵ انتخاب نام سناریوی بعدی و انتخاب قسمت مشخصات نودها



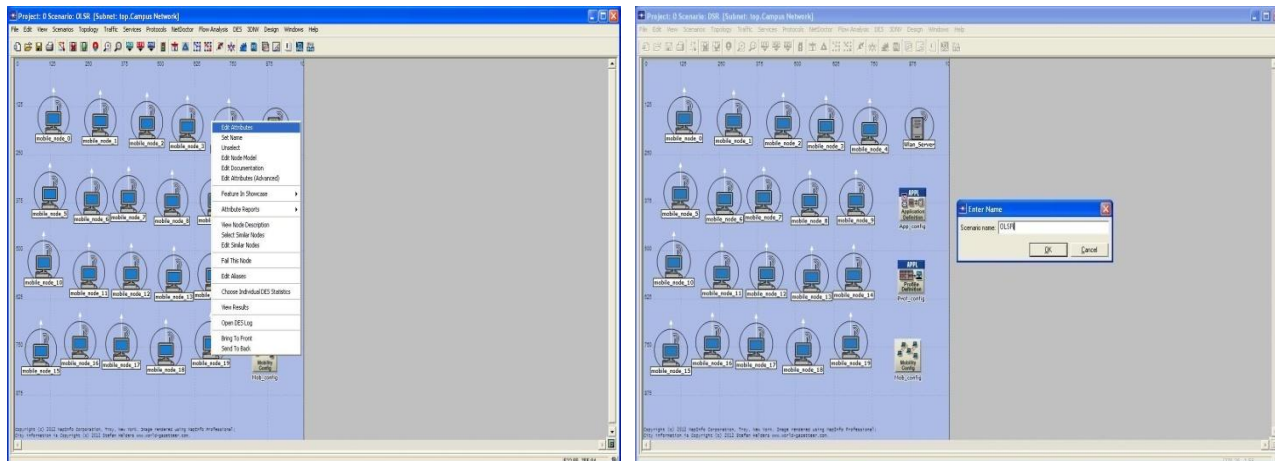
شکل ۵-۱۶ انتخاب پروتکل DSR و انتخاب قسمت انتخاب پروتکل ها برای مشاهده نتایج بعد از شبیه سازی



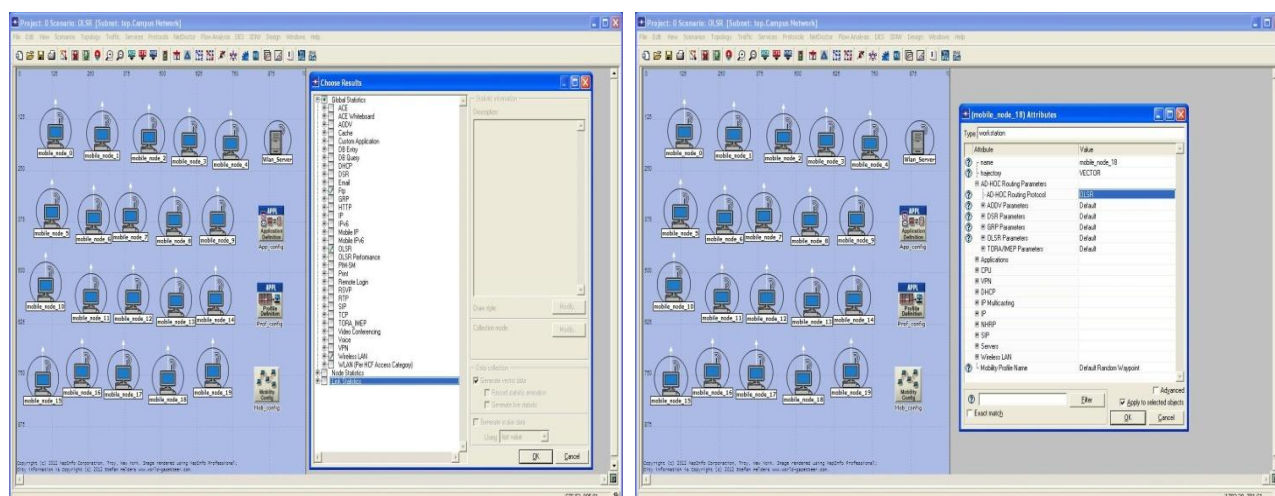
شکل ۵-۱۷ انتخاب پروتکل ها برای مشاهده نتایج بعد از شبیه سازی و انتخاب سناریوی بعدی



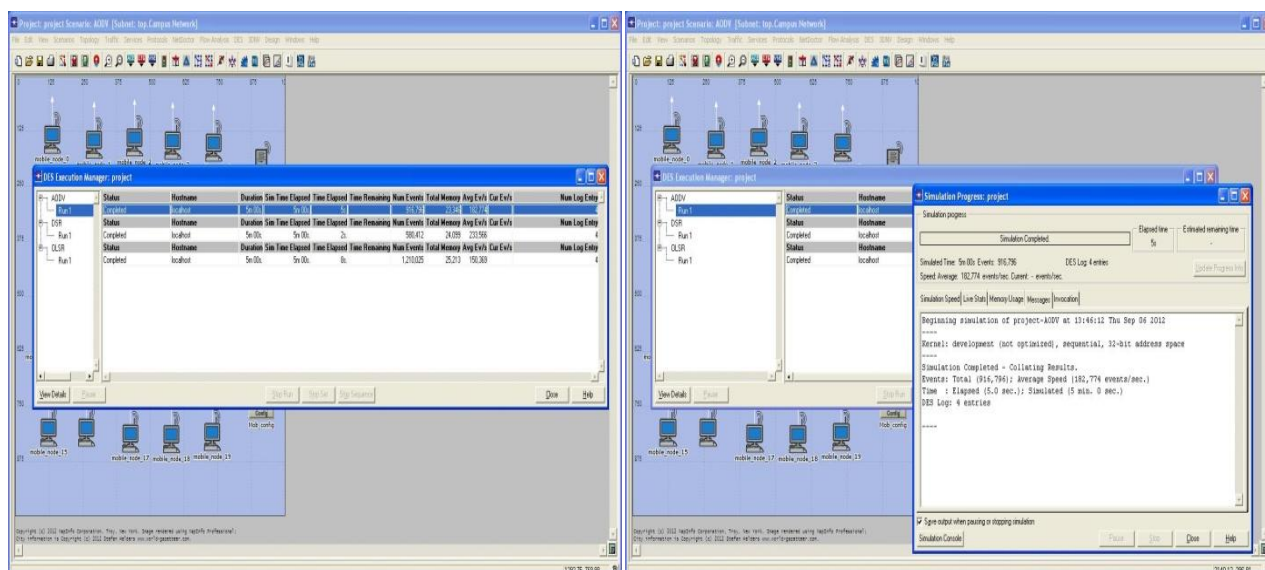
## مقایسه پروتکل های مسیریابی AODV, DSR, OLSR در شبکه های اقتضائی متحرک با نرم افزار شبیه سازی OPNET



شکل ۵-۱۸ انتخاب نام سناریوی بعدی و انتخاب قسمت مشخصات نودها



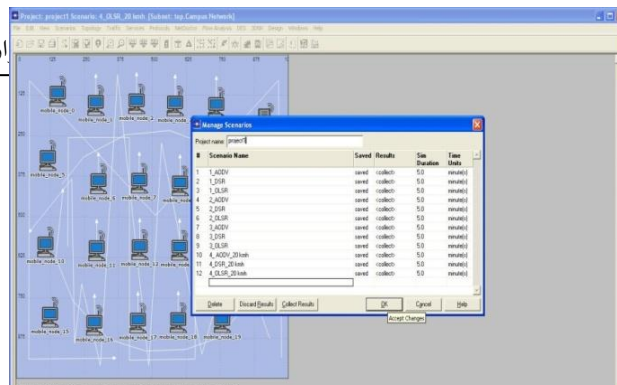
شکل ۵-۱۹ انتخاب پروتکل OLSR و انتخاب قسمت انتخاب پروتکل ها برای مشاهده نتایج بعد از شبیه سازی



شکل ۵-۲۰ اجرای شبیه سازی (۳ سناریو)

ار شیه سازی OPNET

مقایسه پروتکل های مسیر



Project: project1 Scenario: 4\_OLSR\_20 kmh [Subnet: top.Campus Network]

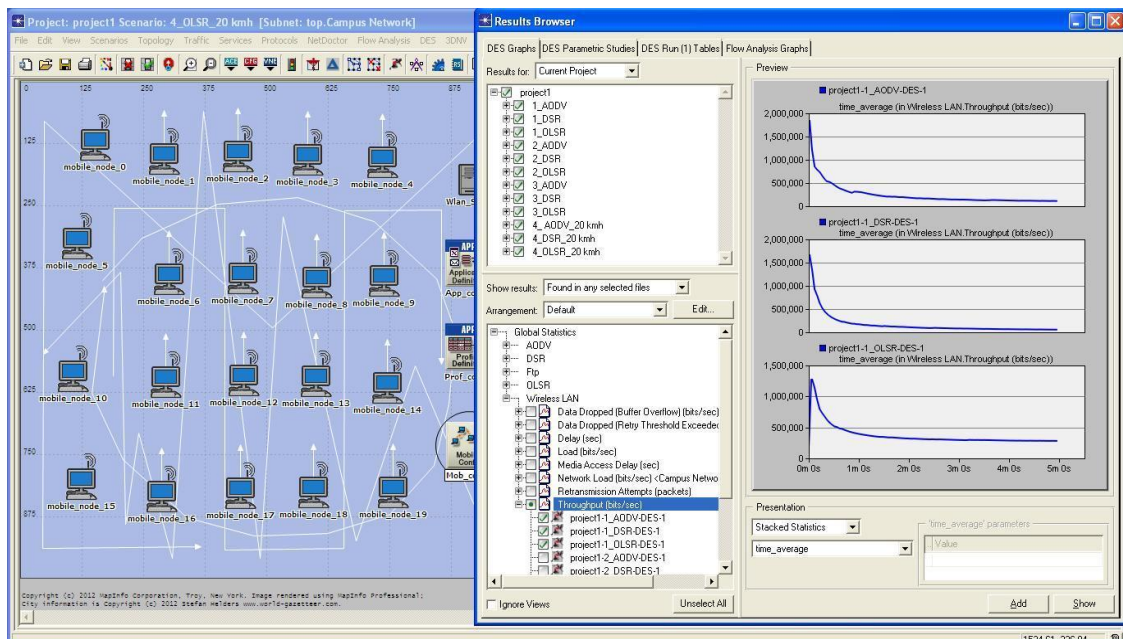
DES Execution Manager: project1

Status	Hostname	Duration	Sim Time Elapsed	Time Elapsed	Time Remaining	Num Events	Total Memory	Avg Ev/s	Cur Ev/s	Num L
Completed	localhost	5m 00s	5m 00s	5m 00s	5m 00s	516,782	23,631	197,898		
Completed	localhost	5m 00s	5m 00s	3s		580,412	23,968	223,838		
Completed	localhost	5m 00s	5m 00s	8s		1,210,025	25,364	157,719		
Completed	localhost	5m 00s	5m 00s	5s		1,025,885	23,281	212,486		
Completed	localhost	5m 00s	5m 00s	2s		567,716	23,676	234,399		
Completed	localhost	5m 00s	5m 00s	8s		1,186,672	25,175	149,794		
Completed	localhost	5m 00s	5m 00s	2s		451,921	21,742	202,292		
Completed	localhost	5m 00s	5m 00s	2s		315,615	21,766	208,326		
Completed	localhost	5m 00s	5m 00s	4s		715,153	22,472	160,600		
Completed	localhost	5m 00s	5m 00s	6s		1,163,105	23,498	191,636		
Completed	localhost	5m 00s	5m 00s	2s		588,034	23,748	230,166		
Completed	localhost	5m 00s	5m 00s	8s		1,227,105	25,338	150,454		

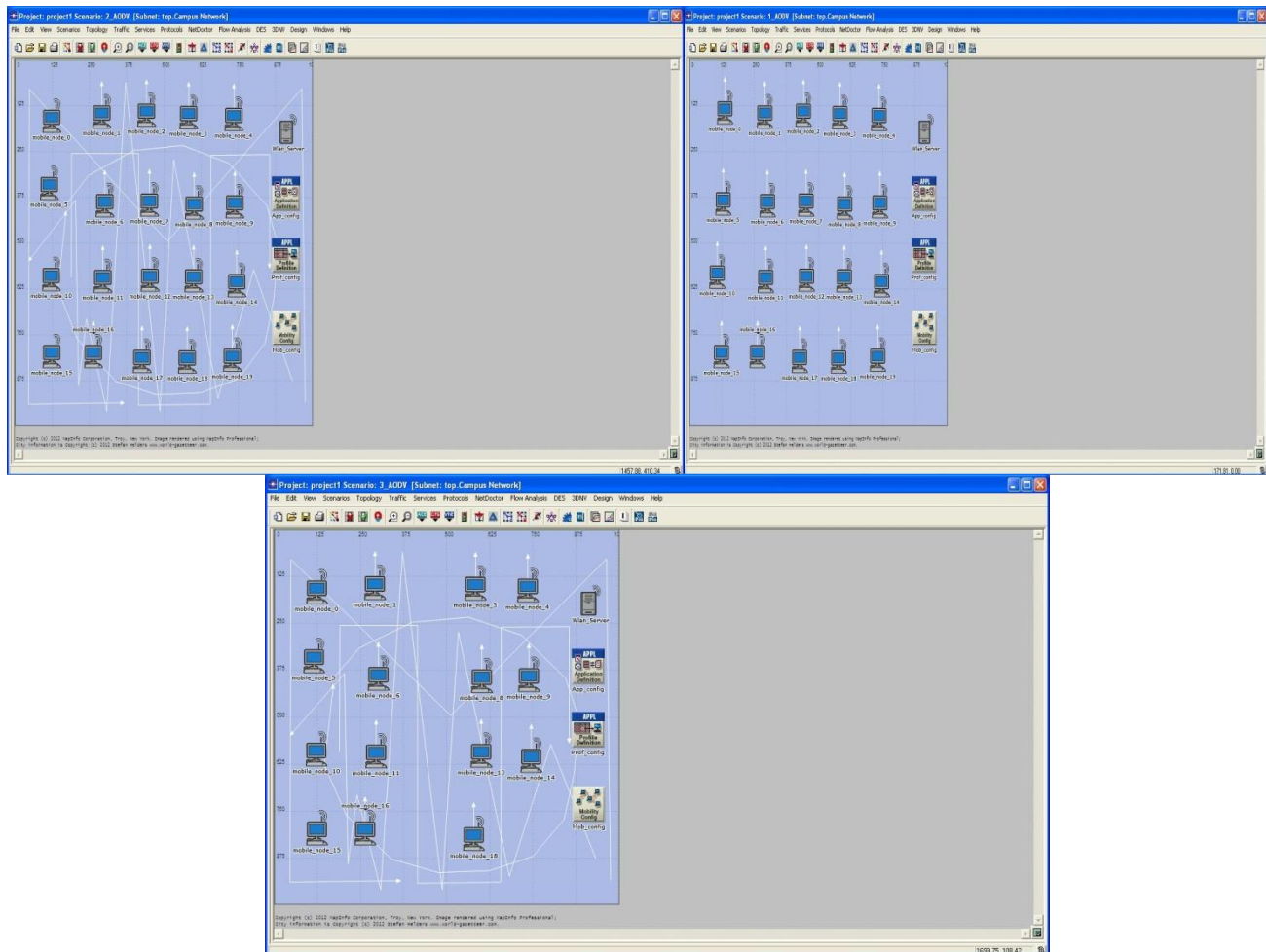
Copyright (c) 2012 HapInfo Corporation, Troy, New York. Image rendered using HapInfo Professional.  
City information is copyright (c) 2012 Stefan Weiders www.world-gazetteer.com.

250.21.16.68

شکل ۵-۲۱ اجرای شبیه سازی (۱۲ سناریو)



شکل ۵-۲۲ مشاهده نتایج شبیه سازی



شکل ۵-۲۳ نمایی از محیط های شبکه

## ۵-۶ نتایج شبیه سازی

این شبیه سازی در مدت ۵ دقیقه صورت گرفته و نتایج این شبیه سازی را بر اساس نمودار `time_average` به شرح ذیل مشاهده خواهید کرد. نتایج شبیه سازی بر اساس پارامترهای زمان تاخیر، میزان سربار شبکه، بار شبکه و توان شبکه می باشد.

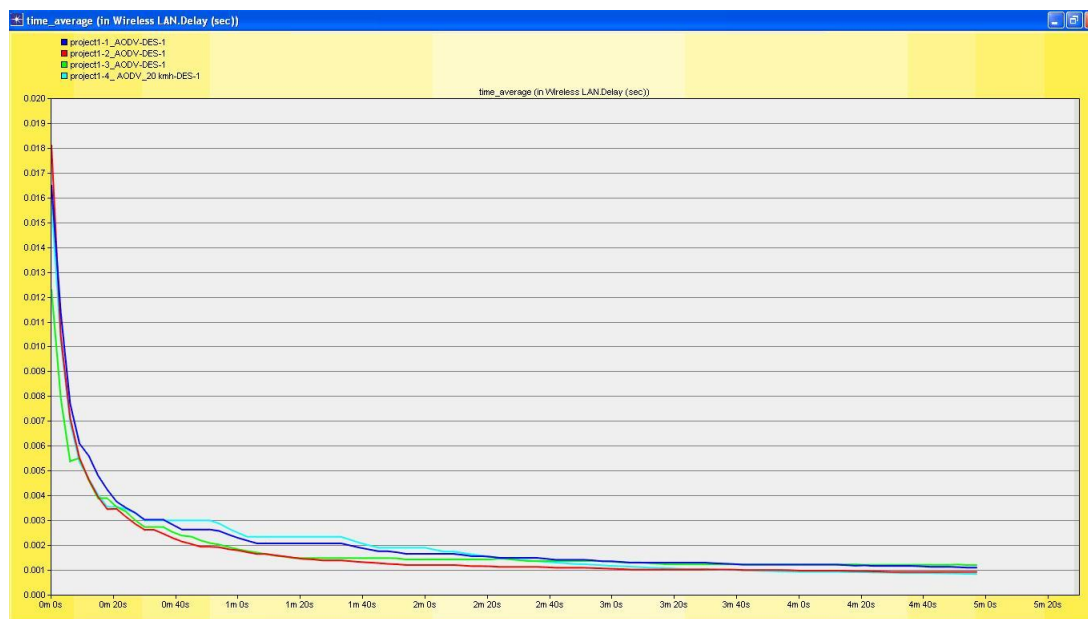
### ۵-۶-۱ نتایج پروتکل AODV در ۴ محیط

در اینجا عملکرد پروتکل AODV بر اساس پارامترهای تاخیر زمان، میزان سربار شبکه، بار شبکه و توان شبکه را بررسی خواهیم کرد. در شکل های زیر محیط اول آبی رنگ، محیط دوم قرمز رنگ و محیط سوم سبز و محیط چهارم آبی روشن می باشد. در شکل زیر میزان تاخیر این پروتکل در ۴ محیط را مشاهده می نمایید.

نمودار محیط اول در ابتدای کار با تاخیر ۰.۰۱۶ ثانیه شروع شده و بعد از طی مدتی مسیریابی به زمان ۰.۰۰۱۰ ثانیه می رسد. در محیط دوم، AODV با تاخیر ۰.۰۱۸ ثانیه شروع به فعالیت کرده و در ادامه به تاخیر ۰.۰۰۰۹ ثانیه می رسد. در محیط سوم که ۱۵ نود متحرک داریم، در ابتدای کار تاخیر ۰.۰۱۲ ثانیه را دارد و در ادامه به ۰.۰۰۱۱ ثانیه می رسد. در محیط چهارم پروتکل با تاخیر ۰.۰۱۵ ثانیه شروع و به تاخیر ۰.۰۰۰۸ ثانیه می رسد. با

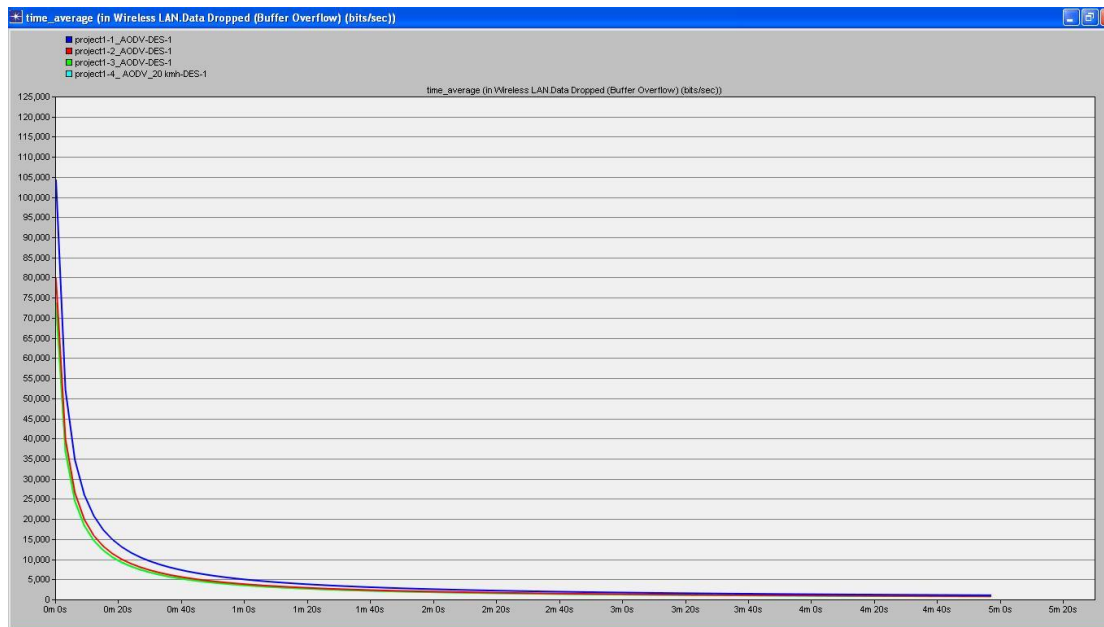


توجه به نمودارها محیط سوم در زمان رو به پایان با تاخیر بیشتر مواجه است و در محیط چهارم با تاخیر کمتر. البته اگر با انحراف معیار بخواهیم صحبت کنیم، محیط سوم با مقدار ۰.۰۰۱۴۸ مقدار کمتری نسبت به بقیه دارد و محیط دوم با مقدار ۰.۰۰۲۱۱ مقدار بیشتری به خود اختصاص داده است. با توجه به نمودار زیر پروتکل در محیط ۴ تاخیر زمان کمتری دارد.



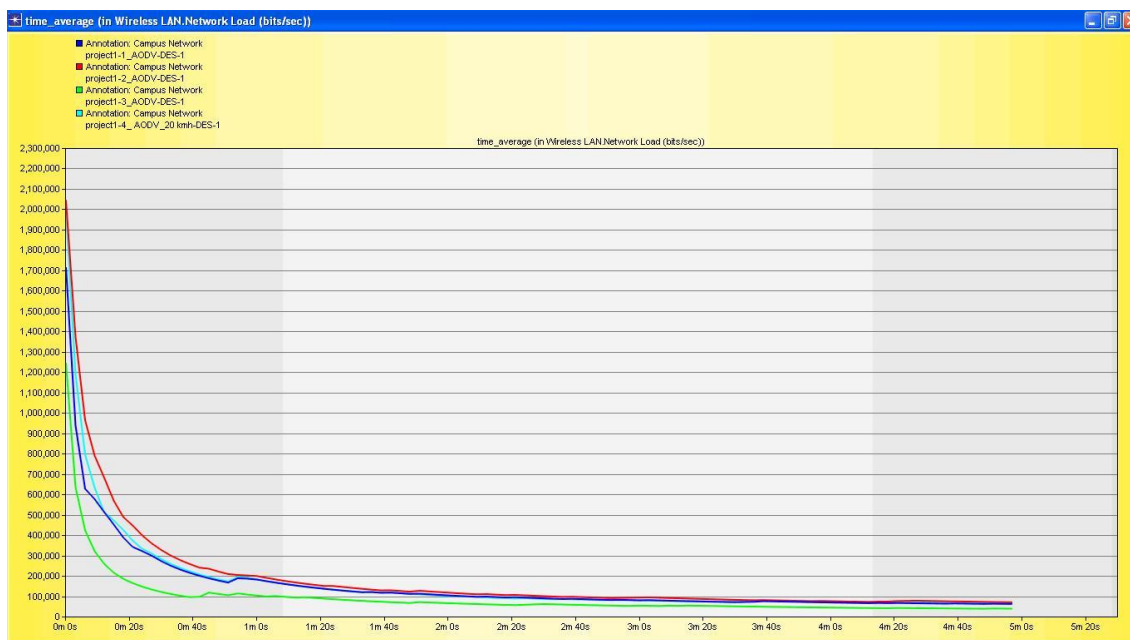
شکل ۵-۲۴ نتایج زمان تاخیر AODV در ۴ محیط

در شکل زیر نتایج میزان سربار در ۴ محیط شبکه را می بینیم. در محیط اول میزان سربار شبکه در ابتدای کار ۱۰۴۴۴۸ bit/s می باشد و در ادامه به ۱۰۴۴ bit/s می رسد. در محیط دوم، در شروع میزان سربار شبکه ۷۳۷۲۸ bit/s می باشد و بعد از طی مدتی به ۷۳۷ bit/s می رسد. در محیط چهارم با ۷۳۷۲۸ bit/s شروع و به ۷۳۷ bit/s می رسد. در اینجا عملکرد پروتکل در محیط سوم و چهارم تقریباً یکسان شد. البته به این نکته باید توجه کرد که محیط سوم با ۱۵ نود می باشد و محیط چهارم با ۲۰ نود و دو برابر سرعت می باشد. در نمودار زیر محیط اول میزان سربار بیشتری دارد.



شکل ۵-۲۵ نتایج میزان سر بار شبکه در AODV در محیط ۴

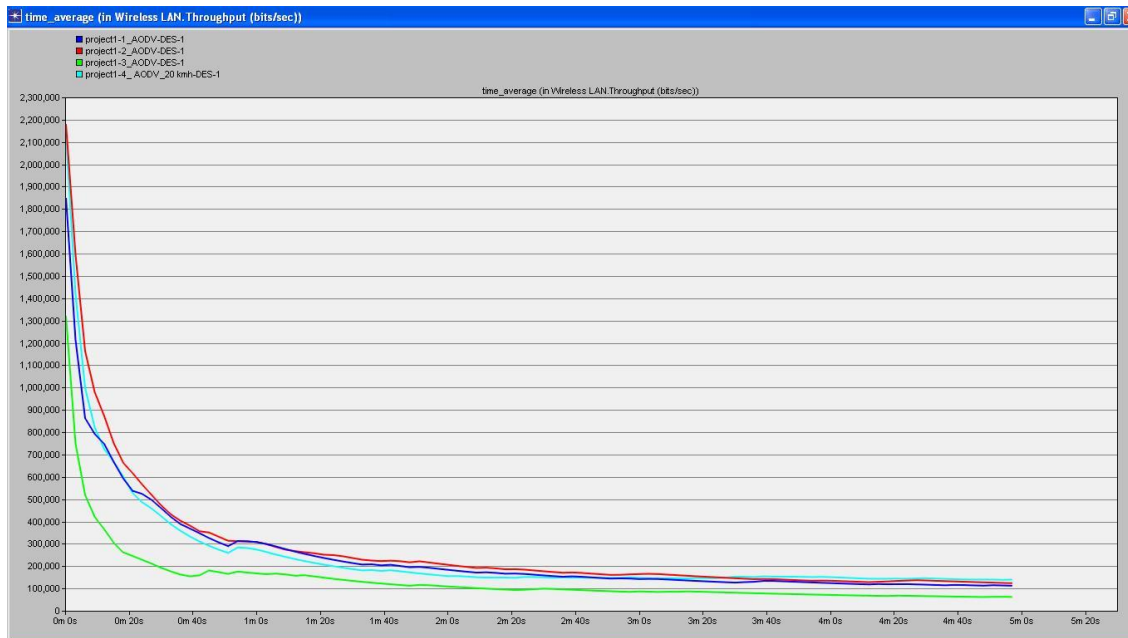
در شکل زیر نتایج بار شبکه را مشاهده می نمایید . با توجه به نمودار، محیط سوم ، در ابتدای کار بار شبکه  $1247338 \text{ bit/s}$  و در ادامه بار شبکه  $38541 \text{ bit/s}$  می باشد . در محیط اول در ابتدای کار بار شبکه  $\text{bit/s}$   $1717248$  می باشد و در ادامه کار بار شبکه به  $61725 \text{ bit/s}$  می رسد . در محیط دوم با  $2044757 \text{ bit/s}$  شروع شده و در ادامه کار به  $69954 \text{ bit/s}$  می رسد . در محیط چهارم نیز بار شبکه با  $1995690 \text{ bit/s}$  شروع شده و به  $64733 \text{ bit/s}$  می رسد . در اینجا محیط سوم بار شبکه کمتری دارد و محیط دوم بار شبکه بیشتری دارد .



شکل ۵-۲۶ نتایج بار شبکه در AODV در محیط ۴

در شکل زیر نتایج توان شبکه را می بینیم . در محیط اول توان شبکه با  $1851445 \text{ bit/s}$  شروع شده و در ادامه به  $112247 \text{ bit/s}$  می رسد . در محیط دوم توان شبکه در ابتدای کار  $2181802 \text{ bit/s}$  و در ادامه به  $123519 \text{ bit/s}$  می رسد . در محیط سوم نیز توان شبکه با  $1320448 \text{ bit/s}$  شروع شده و در ادامه کار به  $61952 \text{ bit/s}$  می رسد .

همچنین در محیط چهارم توان شبکه با  $2129781 \text{ bit/s}$  شروع شده و به مینیمم  $138428 \text{ bit/s}$  ختم می شود. با توجه به نمودار محیط چهارم، توان شبکه بیشتری دارد و محیط سوم توان کمتری دارد.

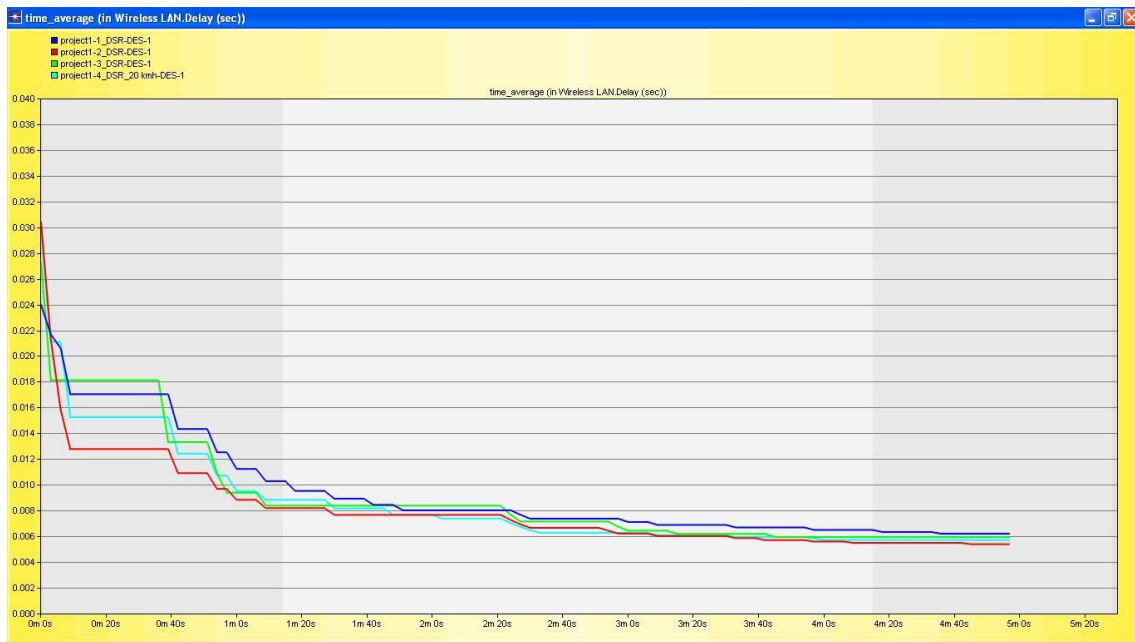


شکل ۵-۲۷ نتایج توان شبکه در AODV در ۴ محیط

با توجه به نتایج می توان گفت که پروتکل در محیط با سرعت حرکت بالاتر نیز مقدار توان بهتری دارد و همچنین تاخیر زمانی کمتری نیز دارد.

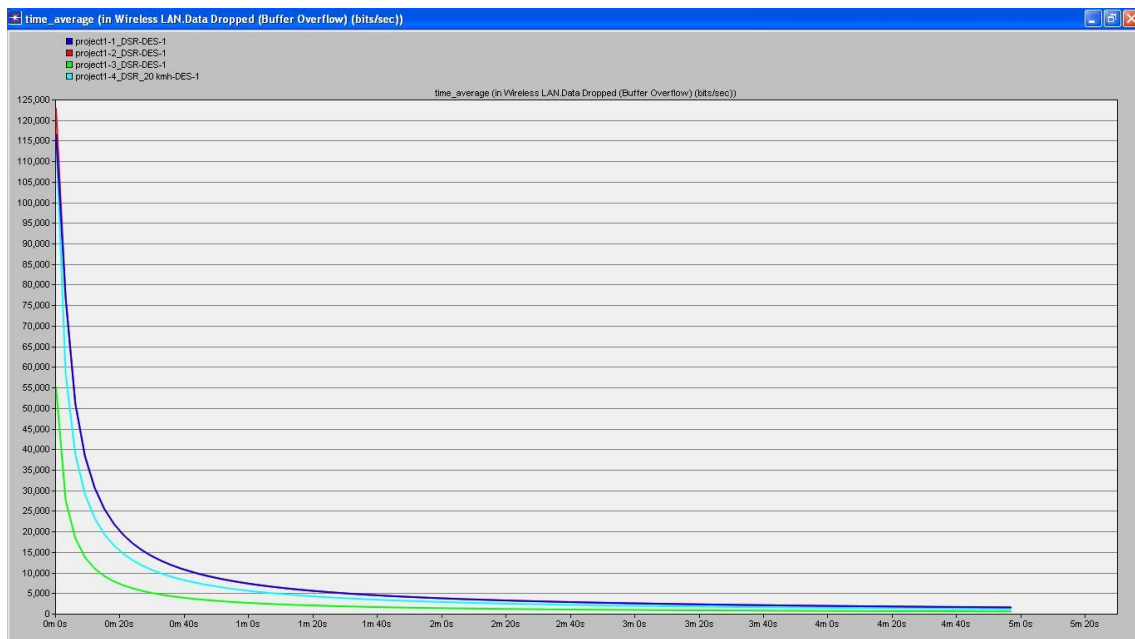
### ۵-۶-۲ نتایج پروتکل DSR در ۴ محیط

در شکل های زیر محیط اول آبی رنگ، محیط دوم قرمز رنگ و محیط سوم سبز و محیط چهارم آبی روشن می باشد. در شکل زیر نتایج شبیه سازی با پارامتر تاخیر زمان در پروتکل DSR را می بینیم. در محیط اول با تاخیر زمانی  $0.024$  ثانیه شروع شده و در ادامه به  $0.062$  ثانیه خواهد رسید. در محیط دوم این تاخیر با  $0.03$  ثانیه شروع شده و به مینیمم  $0.053$  ثانیه می رسد. در محیط سوم در ابتدا با تاخیر  $0.027$  ثانیه و در ادامه با تاخیر  $0.059$  ثانیه مواجه هستیم. در محیط چهارم این تاخیر با  $0.0297$  ثانیه شروع شده و به  $0.057$  ثانیه می رسد. با توجه به نتایج، محیط اول تاخیر بیشتری دارد و محیط دوم تاخیر کمتری دارد.



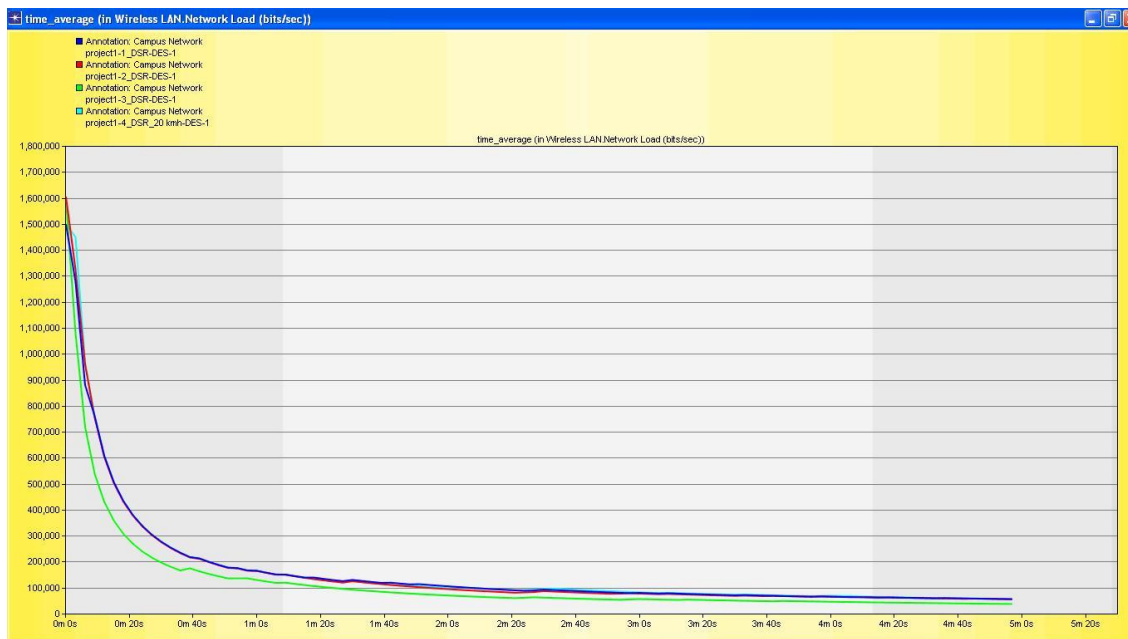
شکل ۵-۲۸ نتایج زمان تاخیر DSR در ۴ محیط

در شکل زیر نتایج میزان سربار شبکه را می بینیم . در محیط اول میزان سربار شبکه با  $116736 \text{ bit/s}$  شروع شده و در ادامه به  $1536 \text{ bit/s}$  می رسد . در محیط دوم سربار شبکه با  $122880 \text{ bit/s}$  شروع و در ادامه به  $552 \text{ bit/s}$  می رسد . در محیط سوم نیز در لحظه شروع  $55296 \text{ bit/s}$  و در ادامه به  $552 \text{ bit/s}$  می رسد . در محیط چهارم سربار شبکه در لحظه شروع  $116736 \text{ bit/s}$  و در ادامه به  $1167 \text{ bit/s}$  می رسد . در اینجا میزان سربار شبکه محیط اول و دوم در ادامه مسیر مشابه هم شدند . در اینجا محیط سوم میزان سربار شبکه کمتری دارد .



شکل ۵-۲۹ نتایج میزان سربار شبکه در DSR در ۴ محیط

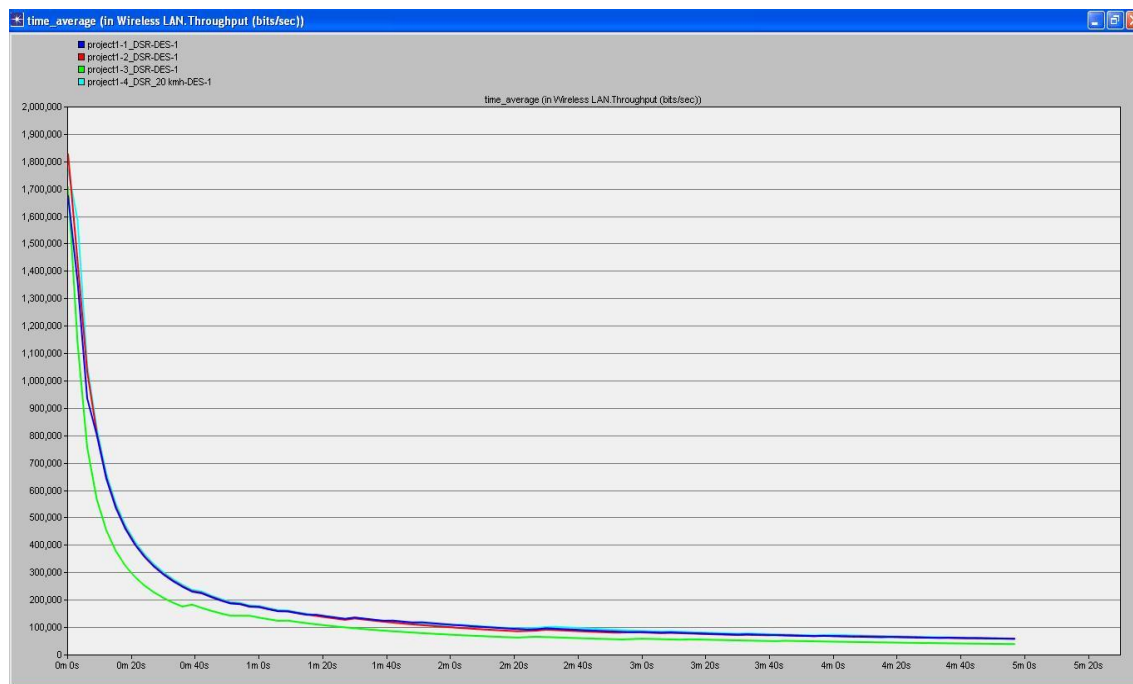
در شکل زیر نتایج بار شبکه را می بینیم . در محیط اول در لحظه شروع بار شبکه  $1498666 \text{ bit/s}$  می باشد و در ادامه به  $55601 \text{ bit/s}$  می رسد . در محیط دوم بار شبکه با  $1606432 \text{ bit/s}$  شروع شده و به  $55353 \text{ bit/s}$  ختم می شود . در محیط سوم بار شبکه با  $1592373 \text{ bit/s}$  شروع و به مینیمم  $36946 \text{ bit/s}$  خواهد رسید . در محیط چهارم در لحظه شروع  $1501013 \text{ bit/s}$  و در ادامه به  $55528 \text{ bit/s}$  خواهد رسید . با توجه به نتایج محیط سوم بار شبکه کمتر و محیط اول بار شبکه بیشتری دارد .



شکل ۵-۳۰ نتایج بار شبکه در DSR در ۴ محیط

در شکل زیر نتایج توان شبکه را می بینیم . در محیط اول توان شبکه در لحظه شروع  $1676618 \text{ bit/s}$  می باشد و در ادامه به  $57274 \text{ bit/s}$  خواهد رسید . در محیط دوم توان شبکه در لحظه شروع  $1828554 \text{ bit/s}$  می باشد و در ادامه به  $57574 \text{ bit/s}$  می رسد . در محیط سوم از  $1707136 \text{ bit/s}$  شروع و به مینیمم  $38094 \text{ bit/s}$  می رسد . در محیط چهارم توان شبکه در لحظه شروع  $1771296 \text{ bit/s}$  و در ادامه به  $58230 \text{ bit/s}$  ختم می شود . با توجه به نتایج محیط سوم توان کمتر و محیط چهارم توان بیشتری دارد .

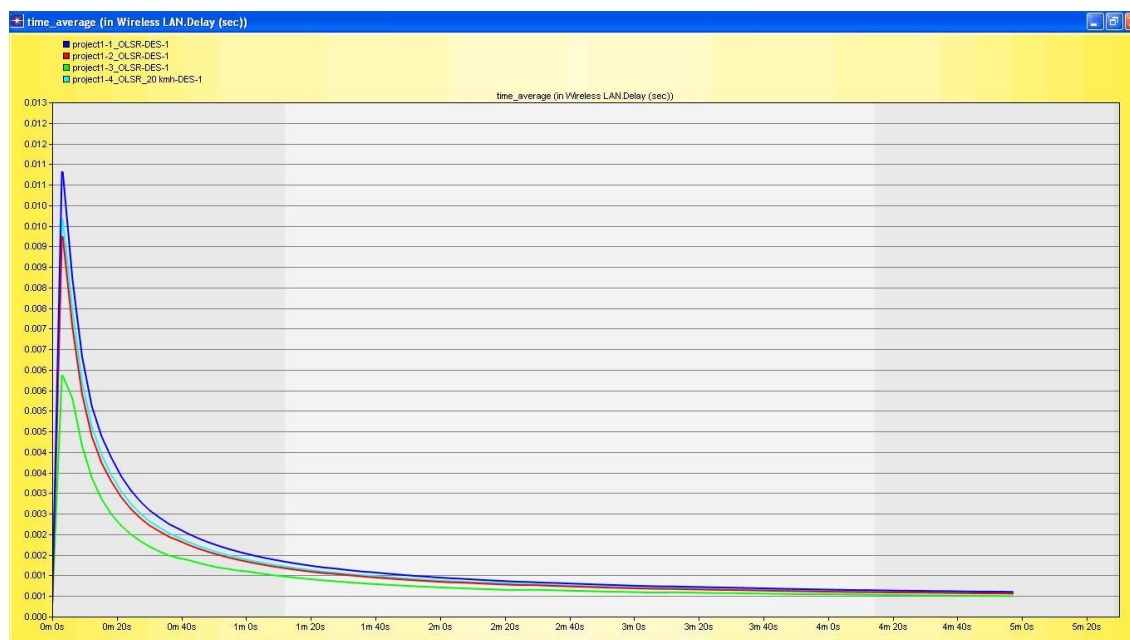




شکل ۳۱-۵ نتایج توان شبکه در DSR در ۴ محیط

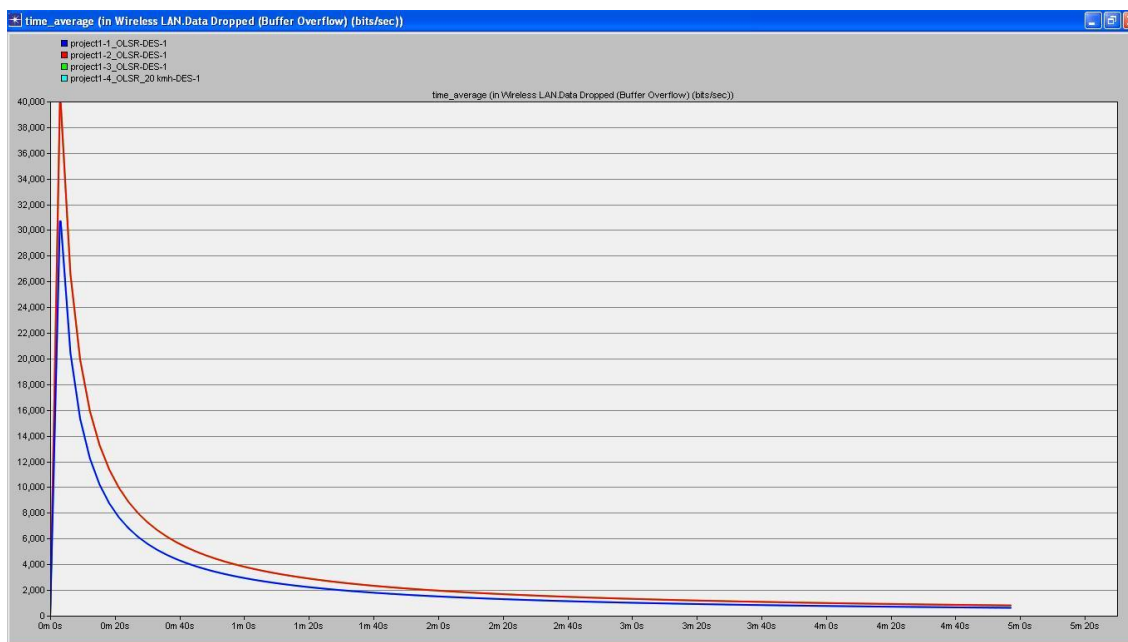
### ۳-۶-۵ نتایج پروتکل OLSR در ۴ محیط

در شکل های زیر محیط اول آبی رنگ ، محیط دوم قرمز رنگ و محیط سوم سبز و محیط چهارم آبی روشن می باشد در شکل زیر نتایج شبیه سازی با پارامتر تاخیر زمان در پروتکل OLSR را می بینیم . در محیط اول در لحظه شروع به ۰.۰۱۰۸ ثانیه تاخیر می رسد و در ادامه به ۰.۰۰۰۶ ثانیه ختم می شود . در محیط دوم به تاخیر ۰.۰۰۹۲ ثانیه می رسد و در ادامه به ۰.۰۰۰۵ ثانیه ختم می شود . در محیط سوم به تاخیر ۰.۰۰۵۸ ثانیه می رسد و در ادامه به تاخیر ۰.۰۰۰۵ ثانیه ختم می شود . در محیط چهارم به تاخیر ۰.۰۰۹۶ ثانیه می رسد و در ادامه به تاخیر ۰.۰۰۰۵ ثانیه ختم می شود . با توجه به نمودار نتایج ، محیط اول تاخیر بیشتری دارد و محیط سوم تاخیر کمتر .



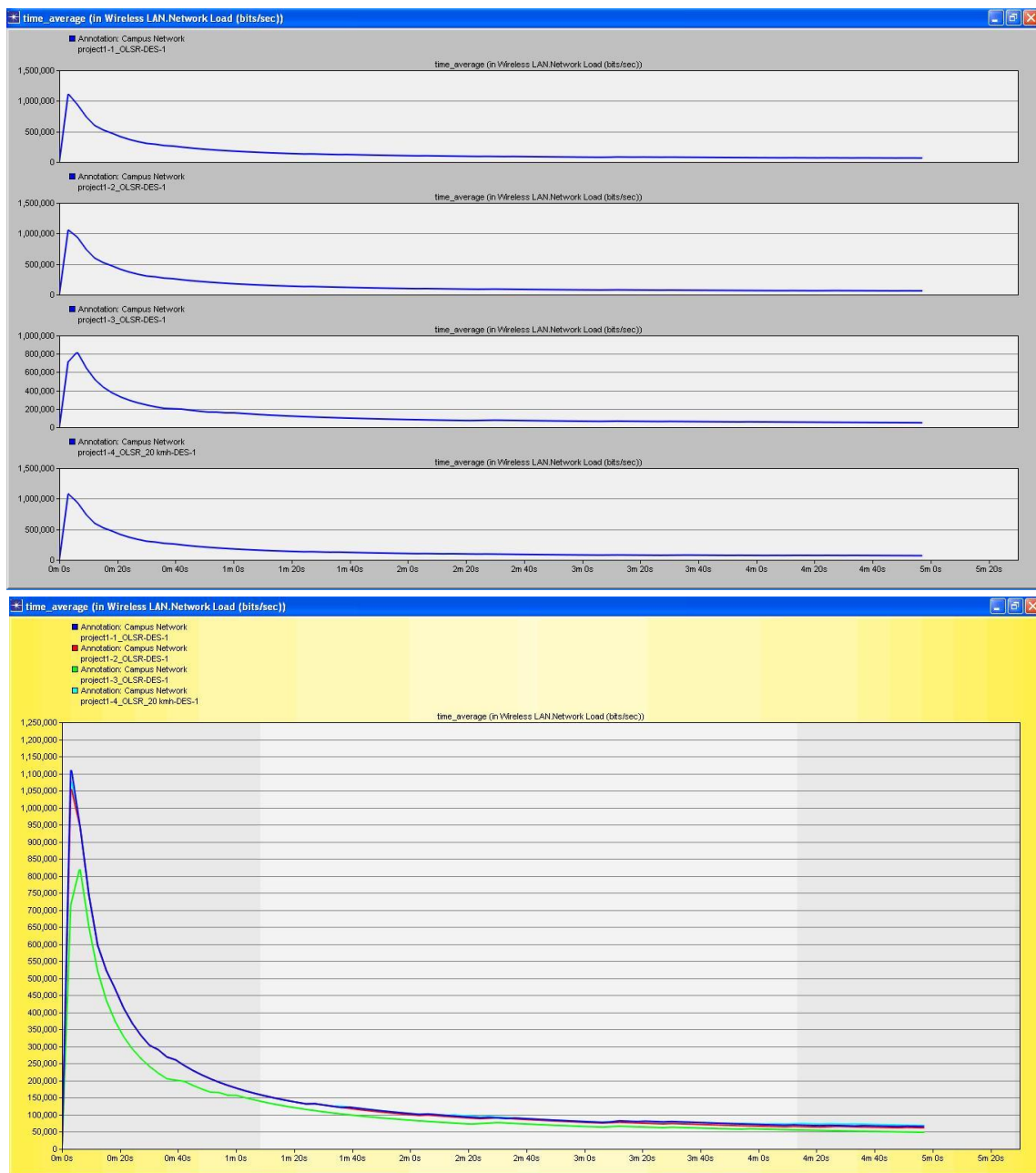
شکل ۳۲-۵ نتایج زمان تاخیر OLSR در ۴ محیط

در شکل زیر نتایج میزان سربار شبکه را مشاهده می نمایید . در محیط اول و چهارم سربار شبکه در ابتدا حدود  $30000 \text{ bit/s}$  می باشد و در ادامه به  $614 \text{ bit/s}$  می رسد . همچنین در محیط دوم و سوم مقدار سربار شبکه در ابتدا حدود  $40000 \text{ bit/s}$  می باشد و در ادامه به مینیمم  $798 \text{ bit/s}$  می رسد . در این نتایج محیط اول و چهارم شبیه به هم و محیط دوم و سوم نیز شبیه هم شدند .



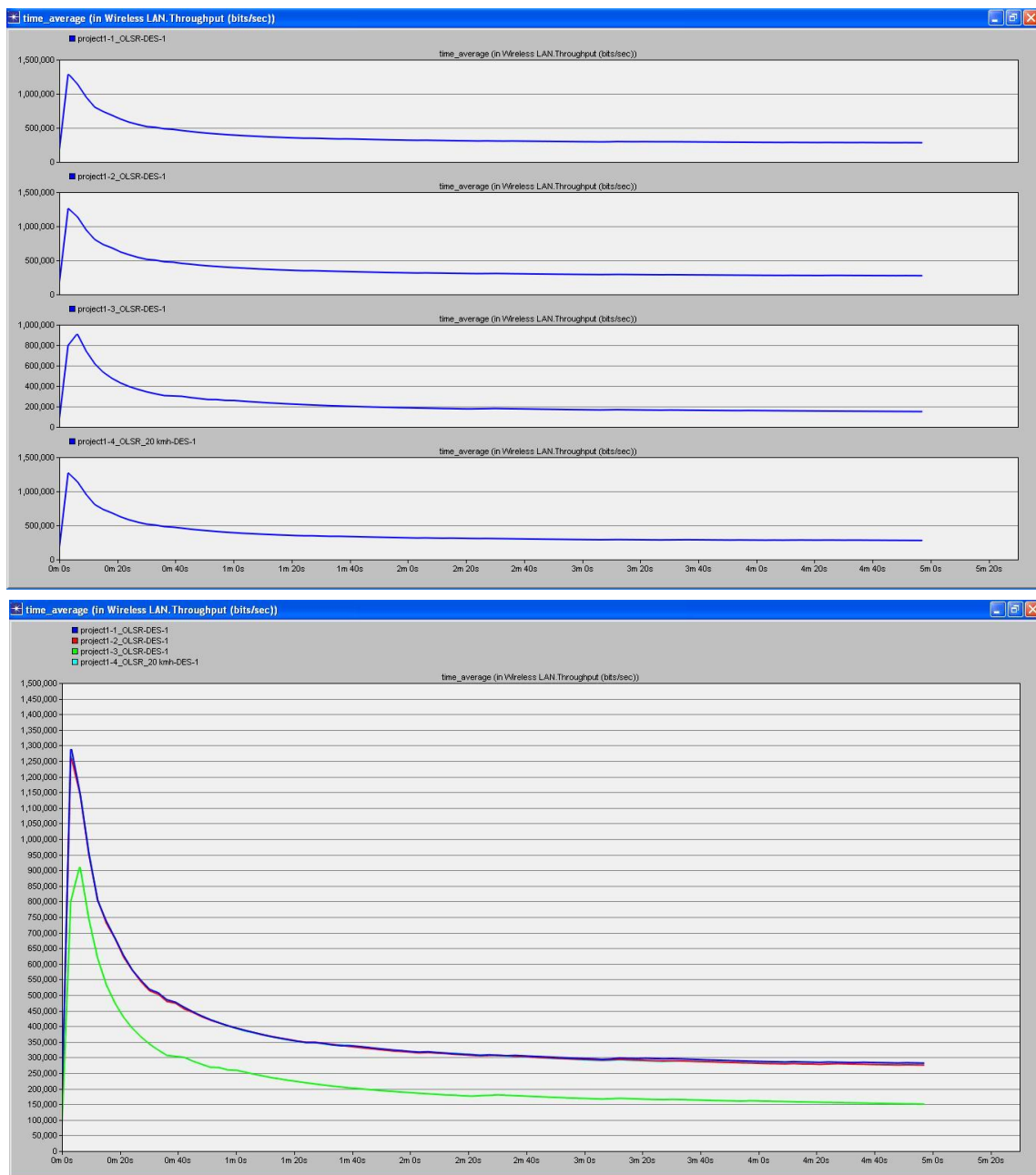
شکل ۵-۳۳ نتایج میزان سربار شبکه در OLSR در ۴ محیط

در شکل زیر نتایج بار شبکه را می بینیم . در ابتدا محیط اول به  $1110853 \text{ bit/s}$  می رسد و در ادامه به  $618 \text{ bit/s}$  ختم می شود . در محیط دوم در ابتدا به  $1055013 \text{ bit/s}$  می رسد و در ادامه به  $61816 \text{ bit/s}$  ختم می شود . در محیط سوم نیز در ابتدا به  $819768 \text{ bit/s}$  می رسد و در ادامه به  $48656 \text{ bit/s}$  ختم می شود . در محیط چهارم در ابتدا به  $1076586 \text{ bit/s}$  می رسد و در ادامه به  $68747 \text{ bit/s}$  ختم می شود . با توجه به نتایج ، محیط چهارم بار شبکه بیشتری دارد و محیط سوم بار شبکه کمتری دارا می باشد .



شکل ۵-۳۴ نتایج بار شبکه در OLSR در ۴ محیط

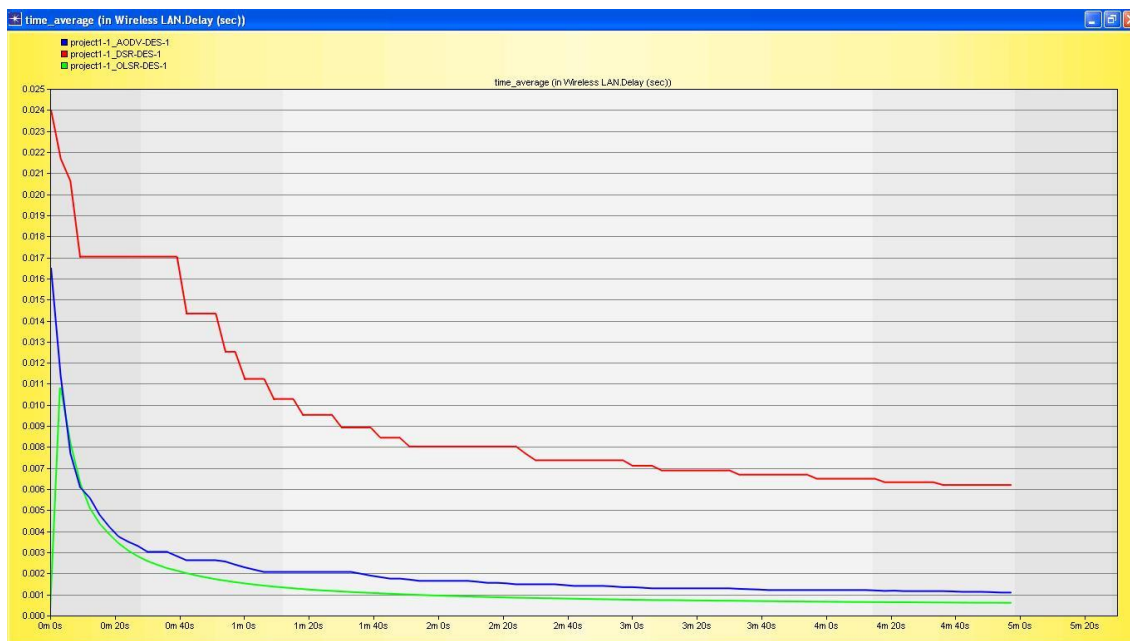
در شکل زیر نتایج توان شبکه را می توان دید . در نمودار اول در لحظه شروع توان شبکه به  $1289034 \text{ bit/s}$  می رسد و در ادامه به  $282142 \text{ bit/s}$  ختم می شود . در محیط دوم نیز در ابتدای کار به  $1259514 \text{ bit/s}$  می رسد و در ادامه به  $275755 \text{ bit/s}$  ختم می شود . در محیط سوم نیز در ابتدای کار به  $910080 \text{ bit/s}$  می رسد و در ادامه به  $1267456 \text{ bit/s}$  می رسد و در ادامه به  $150483 \text{ bit/s}$  ختم می شود . در محیط چهارم ابتدا به  $1267456 \text{ bit/s}$  می رسد و در ادامه به  $279258 \text{ bit/s}$  ختم می شود . با توجه به نتایج ، محیط سوم توان کمتری دارد و محیط اول توان بیشتری دارد .



شکل ۵-۳۵ نتایج توان شبکه در OLSR در ۴ محیط

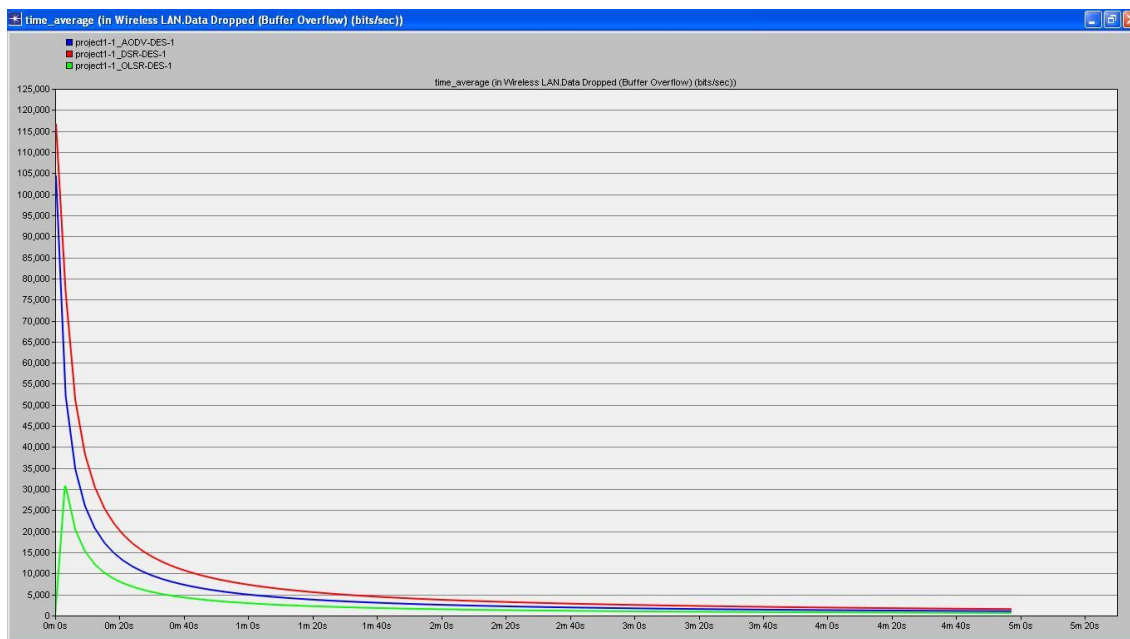
## ۵-۶-۴ نتایج ارزیابی محیط ها با مقایسه سه پروتکل

این شبیه سازی در ۴ محیط مختلف با ۳ پروتکل مسیریابی AODV,DSR,OLSR اجرا شده است. در اینجا در هر شکل، یک محیط شبکه با هر سه پروتکل بر مبنای یک پارامتر بررسی می شود. همان طور که مشاهده می نمایید، در شکل زیر میزان تاخیر در محیط اول بررسی شده که بر اساس این نمودارها مشخص می شود که پروتکل DSR دارای بیشترین تاخیر و پروتکل OLSR دارای کمترین زمان تاخیر می باشد. همچنین AODV نسبت به DSR نیز تاخیر کمتری دارد و بهتر عمل می کند.



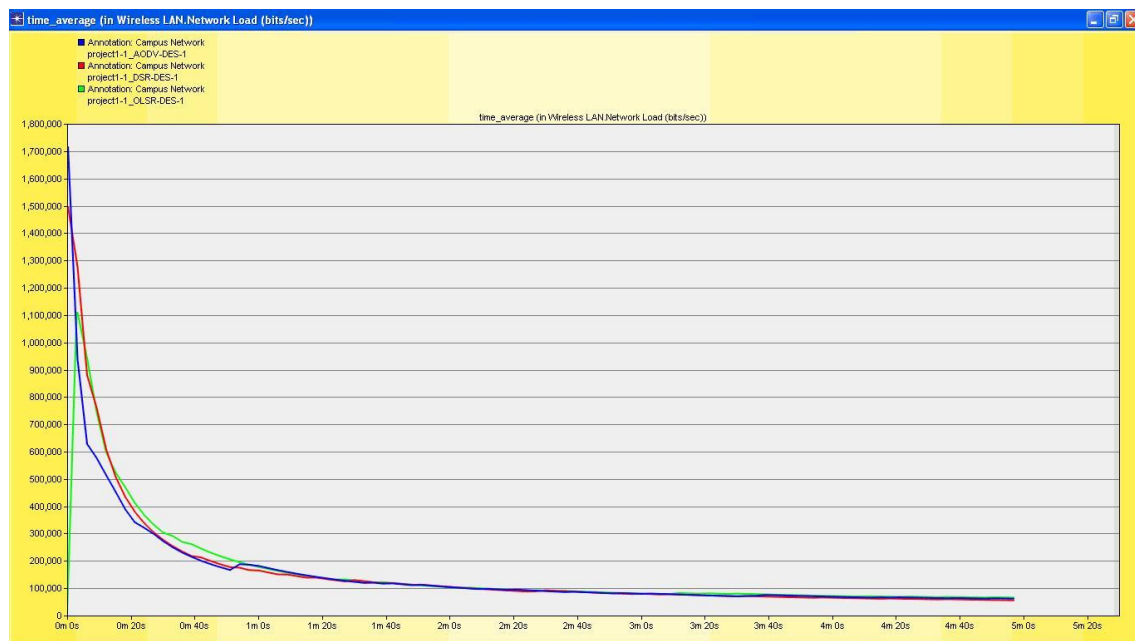
شکل ۵-۳۶ نتایج میزان تاخیر در محیط ۱ – AODV,DSR,OLSR

در شکل زیر میزان سربار شبکه در محیط ۱ بررسی شده که پروتکل DSR دارای بیشترین میزان سربار شبکه و پروتکل OLSR دارای کم ترین میزان سربار شبکه می باشد .



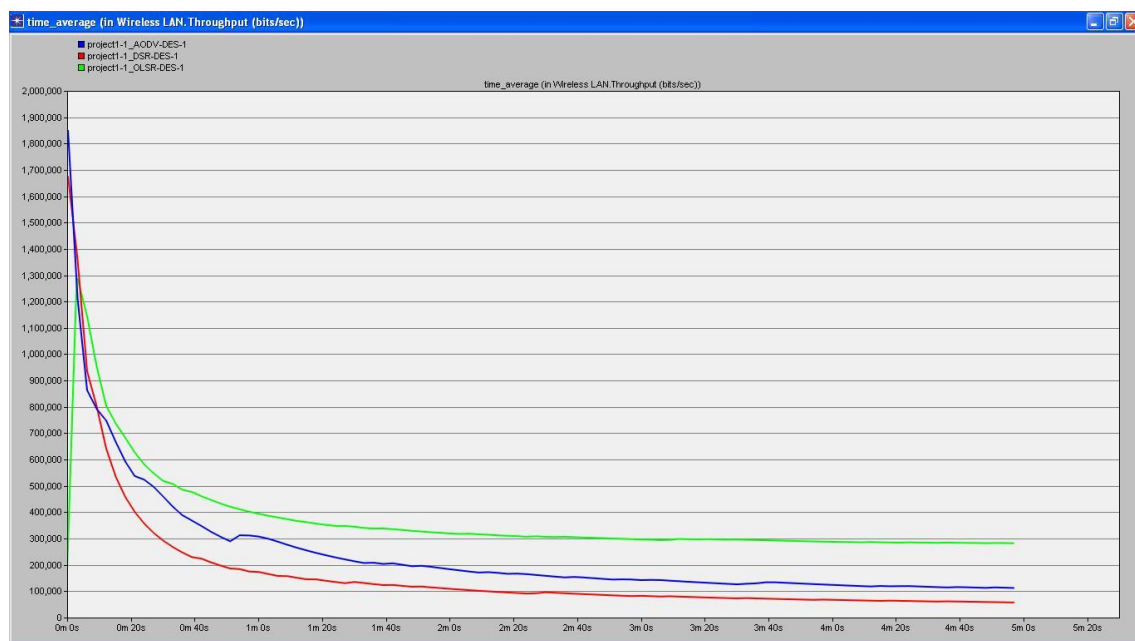
شکل ۵-۳۷ نتایج میزان سربار شبکه در محیط ۱ – AODV,DSR,OLSR

در شکل زیر بار شبکه در محیط ۱ بررسی شده که با توجه به نتایج نمودار در امتداد مسیر ، پروتکل OLSR دارای بار شبکه بیشتر و پروتکل DSR بار شبکه کمتری دارا می باشد .



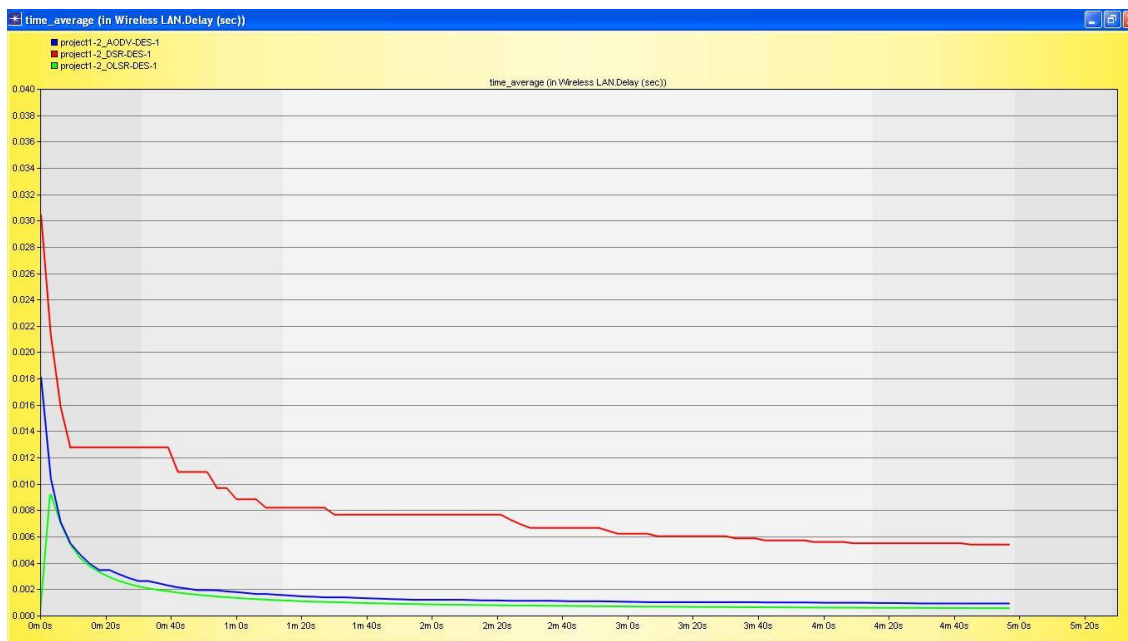
شکل ۵-۳۸ نتایج بار شبکه در محیط ۱ - AODV,DSR,OLSR

در شکل زیر توان شبکه در محیط ۱ بررسی شده که با توجه به نتایج نمودار، پروتکل OLSR دارای توان بیشتر و نیز پروتکل DSR دارای توان کمتری می باشد. AODV نیز توان بهتری نسبت به DSR دارد.



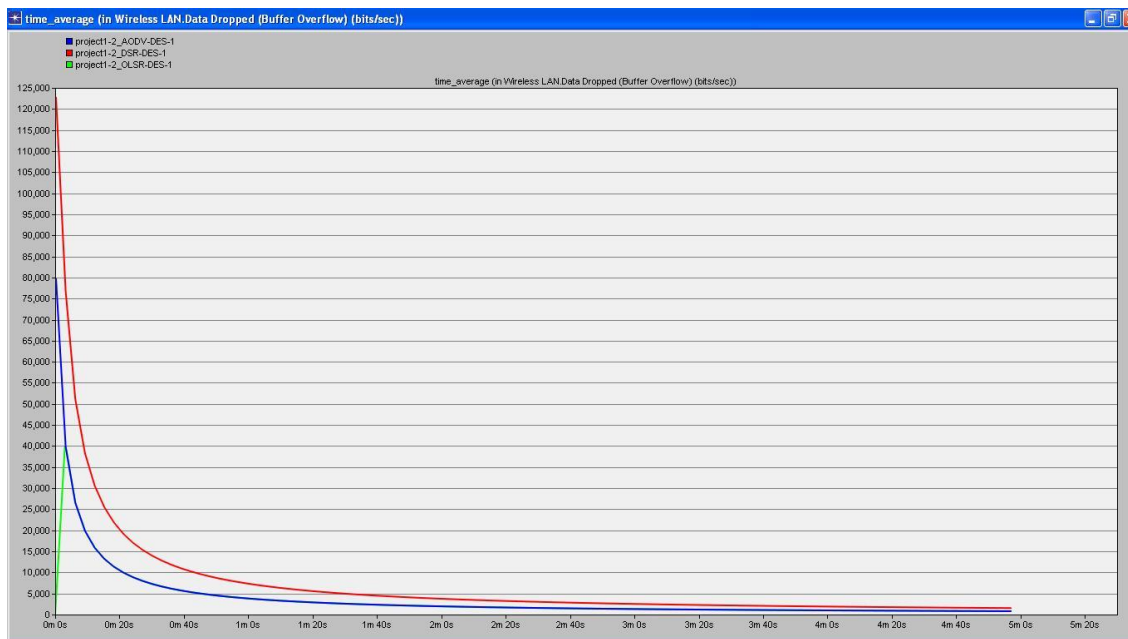
شکل ۵-۳۹ نتایج توان شبکه در محیط ۱ - AODV,DSR,OLSR

در شکل زیر میزان تاخیر در محیط ۲ مورد بررسی قرار گرفته که مشخص می نماید پروتکل DSR دارای بیشترین زمان تاخیر و پروتکل OLSR دارای کمترین زمان تاخیر می باشد. AODV نیز بهتر از DSR میباشد.



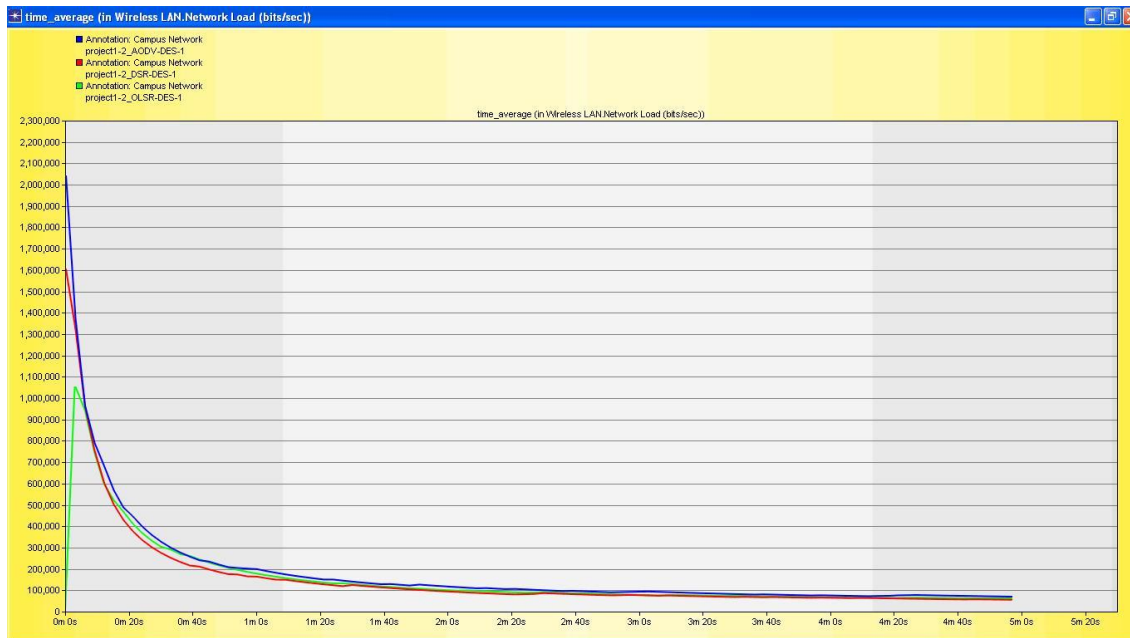
شکل ۵-۴ نتایج میزان تاخیر در محیط ۲ - AODV, DSR, OLSR

در شکل زیر میزان سربار شبکه در محیط ۲ بررسی شده که مشخص می نماید پروتکل DSR دارای بیشترین میزان سربار شبکه می باشد و پروتکل OLSR و پروتکل AODV در امتداد مسیر نمودار، نتیجه یکسانی دارند. البته با این تفاوت که OLSR در ابتدای کار به  $39936 \text{ bit/s}$  می رسد و در ادامه به  $798 \text{ bit/s}$  ختم می شود. ولی AODV از  $79872 \text{ bit/s}$  شروع شده و در ادامه به  $798 \text{ bit/s}$  می رسد.



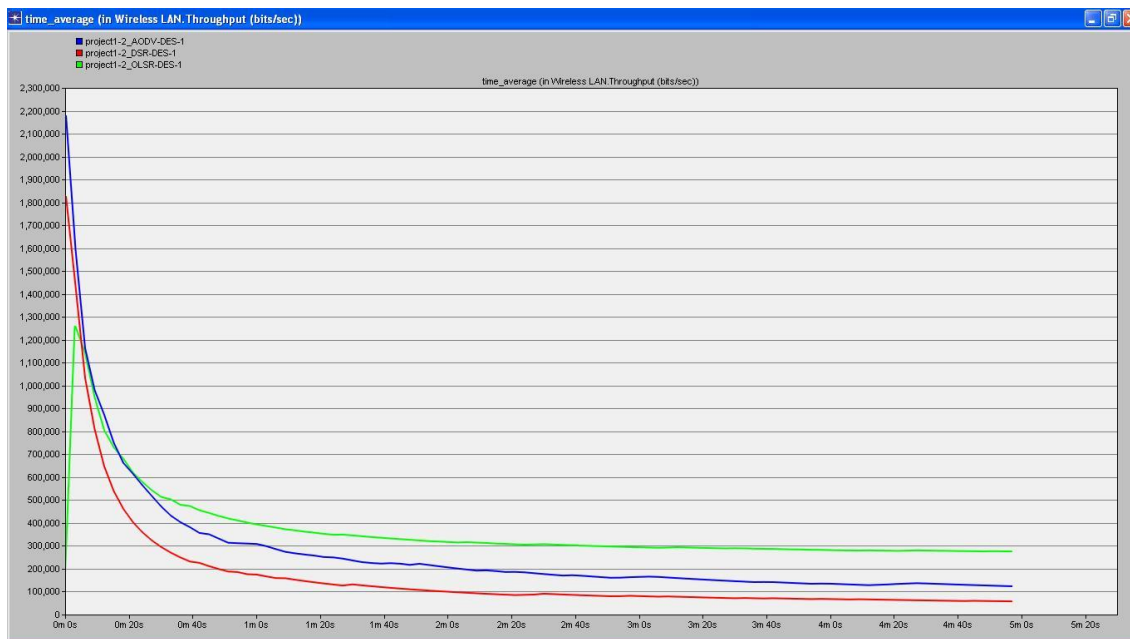
شکل ۵-۴ نتایج میزان سربار شبکه در محیط ۲ - AODV, DSR, OLSR

در شکل زیر بار شبکه در محیط ۲ مورد بررسی قرار گرفته که مشخص می کند ، پروتکل AODV نسبت به بقیه بار شبکه بیشتری داشته و پروتکل DSR بار کمتری دارد .



شکل ۵-۴۲ نتایج بار شبکه در محیط ۲ - AODV,DSR,OLSR

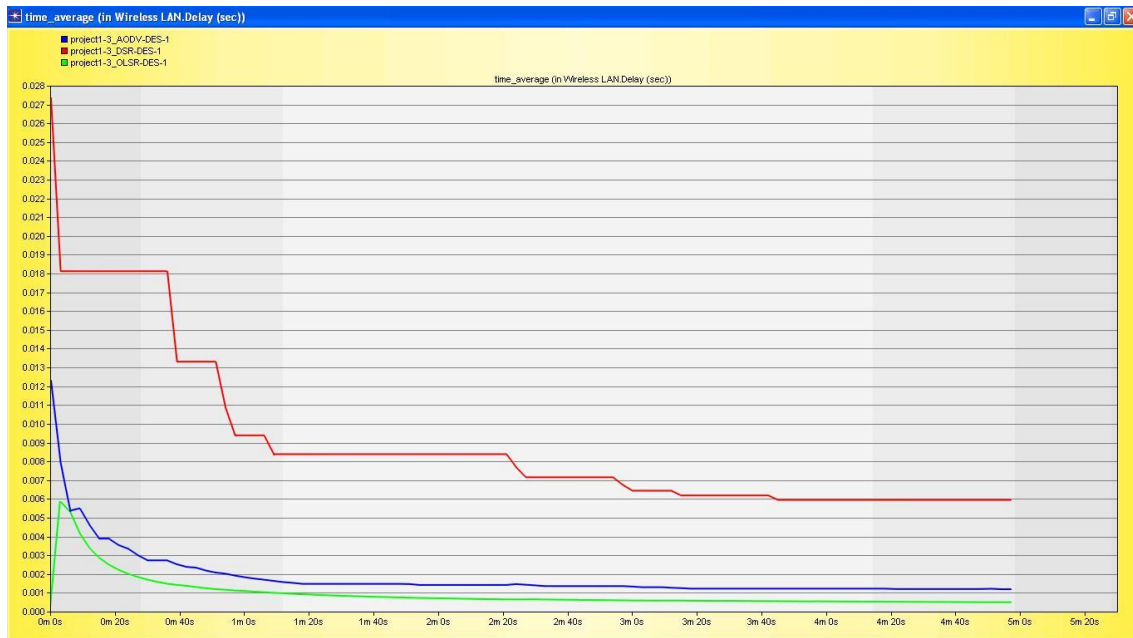
در شکل زیر توان شبکه در محیط ۲ مورد بررسی قرار گرفته که حاوی عملکرد بهتر OLSR می باشد. در اینجا OLSR دارای توان بیشتر و DSR دارای توان کمتری می باشد . AODV نیز بهتر از DSR می باشد .



شکل ۵-۴۳ نتایج توان شبکه در محیط ۲ - AODV,DSR,OLSR

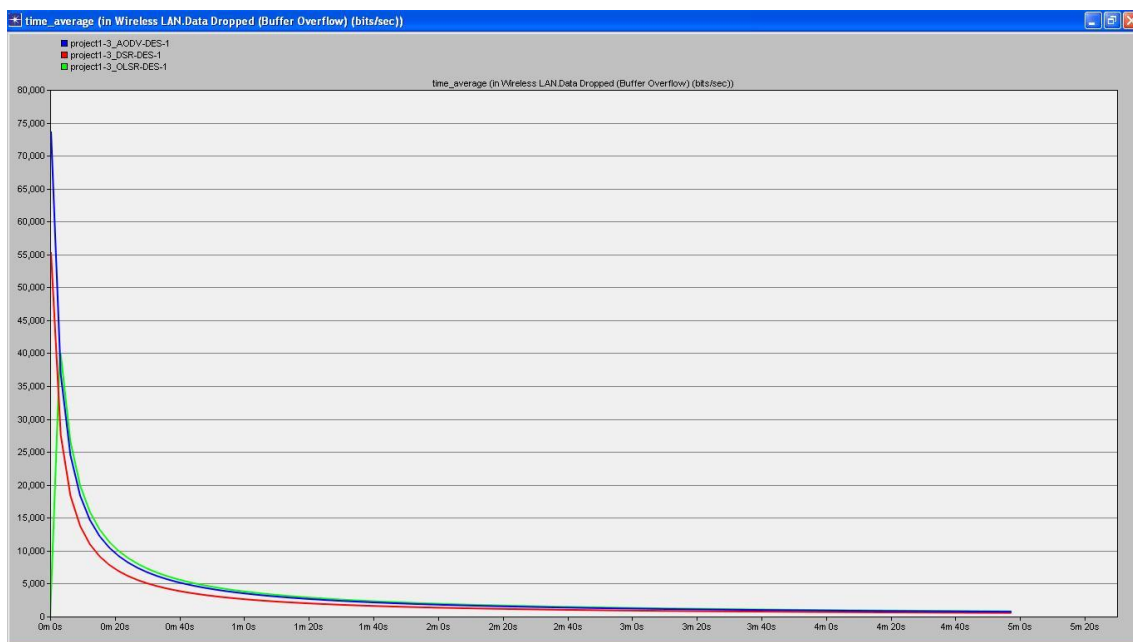


در شکل زیر میزان تاخیر در محیط ۳ بررسی شده که مشخص می کند پروتکل DSR دارای بیشترین تاخیر بوده و پروتکل OLSR تاخیر کمتری دارد. AODV نیز تاخیر کمتری نسبت به DSR دارد.



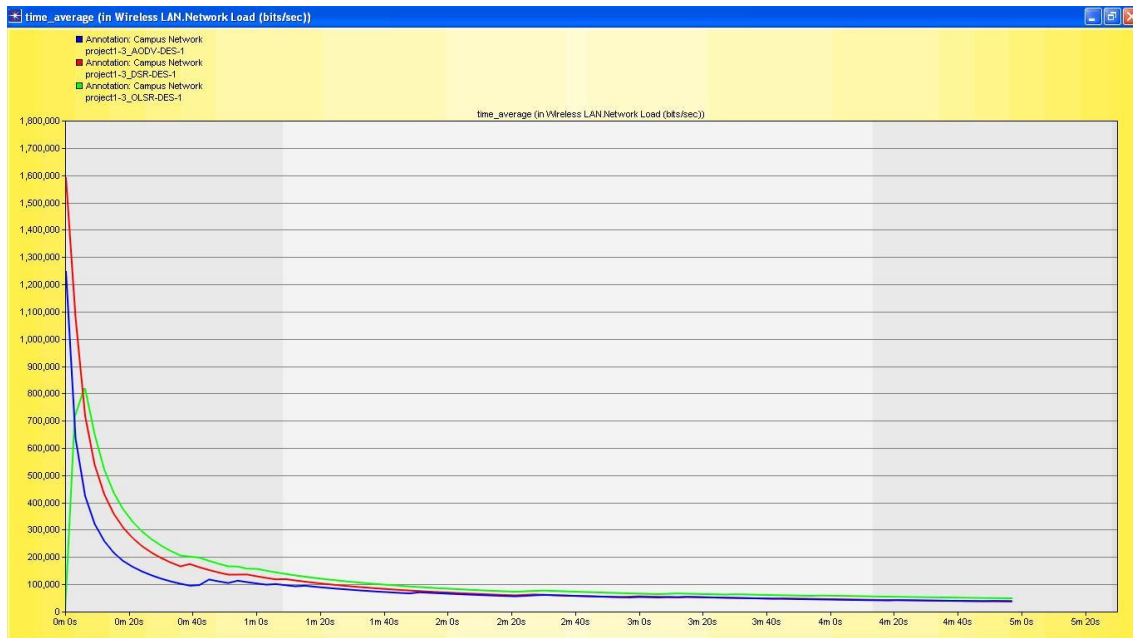
شکل ۵-۴۴ نتایج میزان تاخیر در محیط ۳ - AODV, DSR, OLSR

در شکل زیر میزان سربار شبکه در محیط ۳ بررسی شده که با توجه به نمودار نتایج، پروتکل DSR دارای میزان سربار کمتر (۵۵۲ bit/s) و پروتکل OLSR (۷۹۸ bit/s) میزان سربار بیشتری دارد. البته نتایج خیلی به یکدیگر نزدیک می باشد AODV نیز به ۷۳۷ bit/s می رسد.



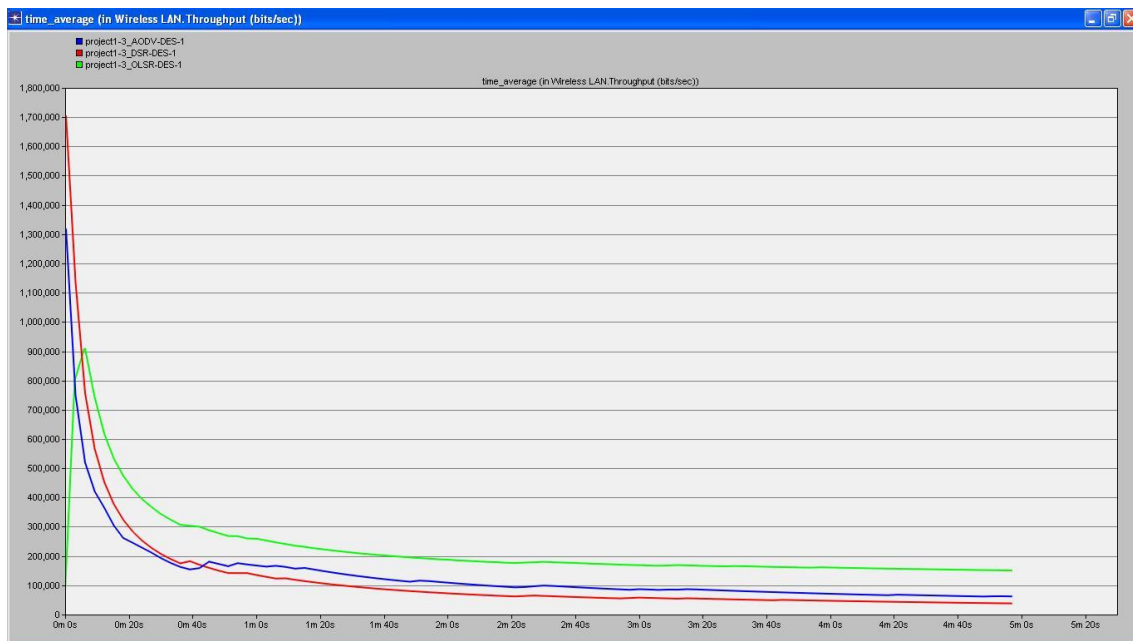
شکل ۵-۴۵ نتایج میزان سربار شبکه در محیط ۳ - AODV, DSR, OLSR

در شکل زیر بار شبکه در محیط ۳ بررسی شده که با توجه به نتایج، پروتکل OLSR بار شبکه بیشتری دارد و پروتکل DSR نیز بار کمتر. البته نتیجه DSR با AODV به یکدیگر خیلی نزدیک می باشد.



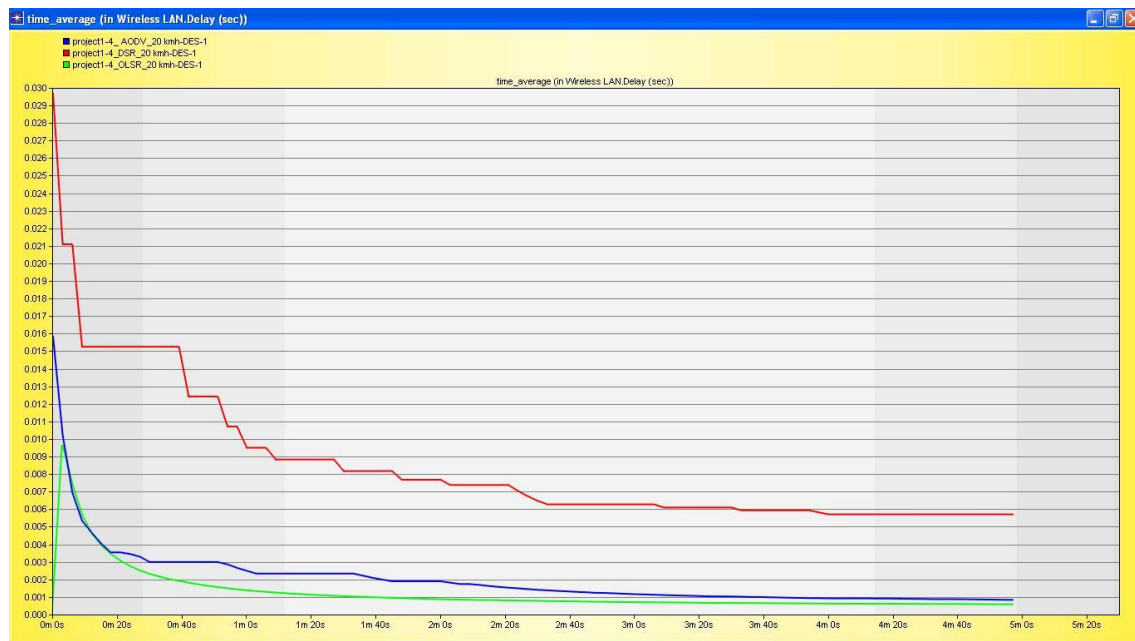
شکل ۵-۴ نتایج بار شبکه در محیط ۳ - AODV, DSR, OLSR

در شکل زیر توان شبکه در محیط ۳ بررسی شده که بیانگر عملکرد بهتر پروتکل OLSR می باشد. همچنین پروتکل DSR عملکرد پایین تری دارد. همچنین AODV نسبت به DSR دارای مقدار توان بهتری می باشد.



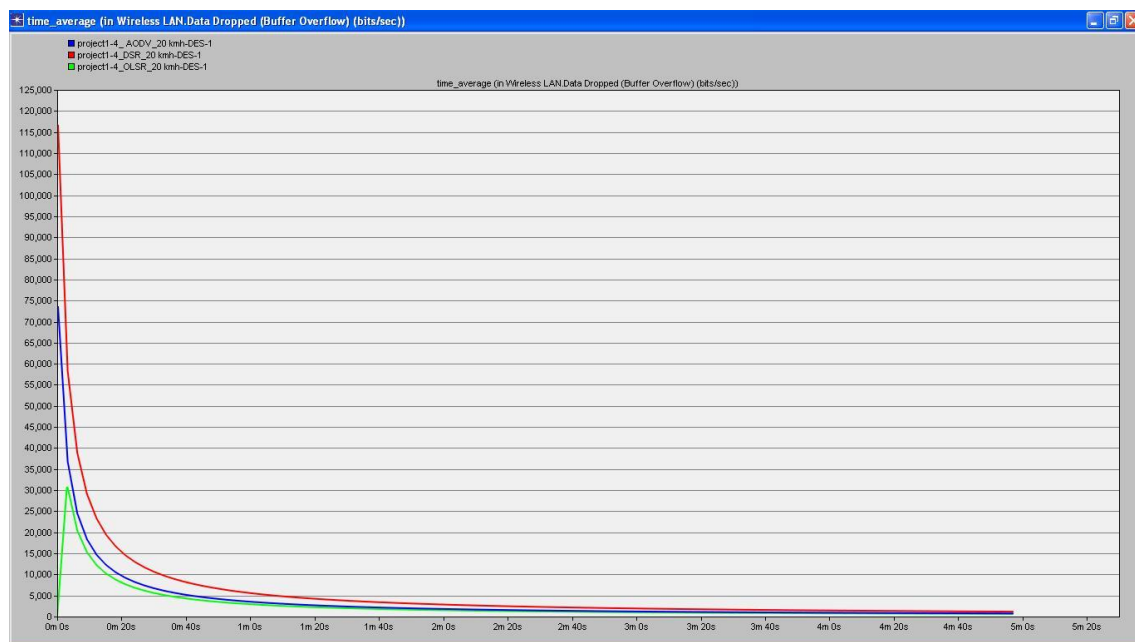
شکل ۵-۴ نتایج توان شبکه در محیط ۳ - AODV, DSR, OLSR

در شکل زیر زمان تاخیر در محیط ۴ بررسی شده که مشخص می کند پروتکل DSR دارای بیشترین تاخیر و پروتکل OLSR دارای کمترین تاخیر زمانی می باشد. همچنین AODV نیز تاخیر کمتری نسبت به DSR دارد



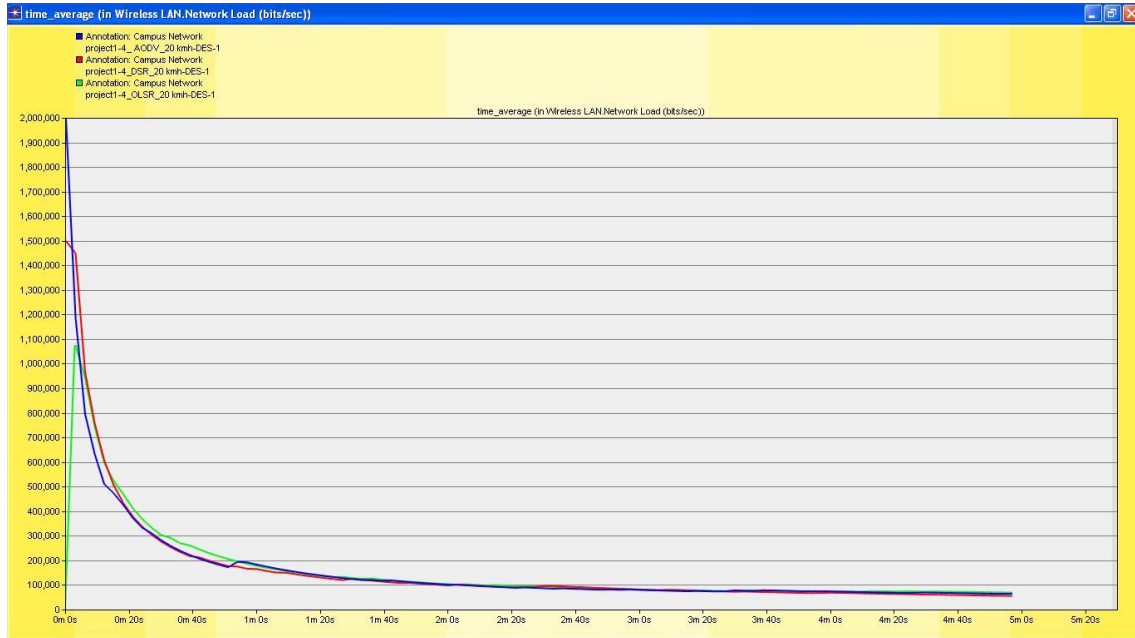
شکل ۴-۵ نتایج میزان تاخیر در محیط ۴ - AODV,DSR,OLSR

در شکل زیر میزان سربار شبکه در محیط ۴ بررسی شده که بیانگر میزان سربار بیشتر در DSR و میزان سربار کمتر در OLSR می باشد .



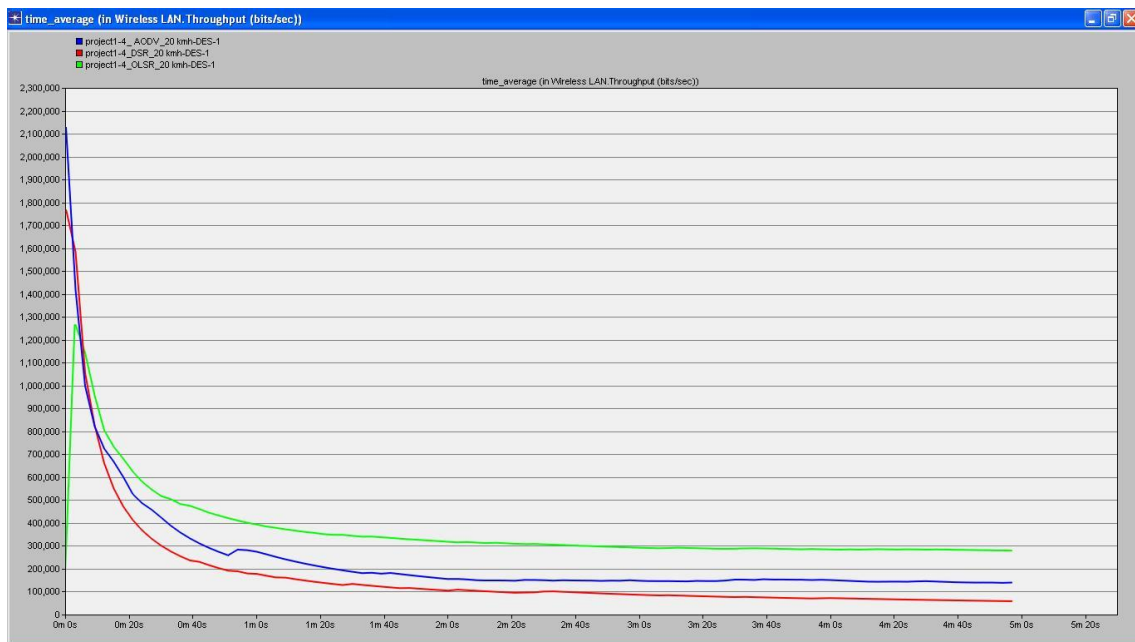
شکل ۴-۹ نتایج میزان سربار شبکه در محیط ۴ - AODV,DSR,OLSR

در شکل زیر بار شبکه در محیط ۴ بررسی شده که با توجه به نزدیکی نمودارهای نتایج این گونه می توان تصمیم گرفت که پروتکل DSR بار شبکه کمتری دارد ( البته با مشاهده امتداد مسیر نمودار) و پروتکل OLSR نیز بار شبکه بیشتری دارد . البته با ذکر این نکته که داده ها نزدیک به هم هستند .



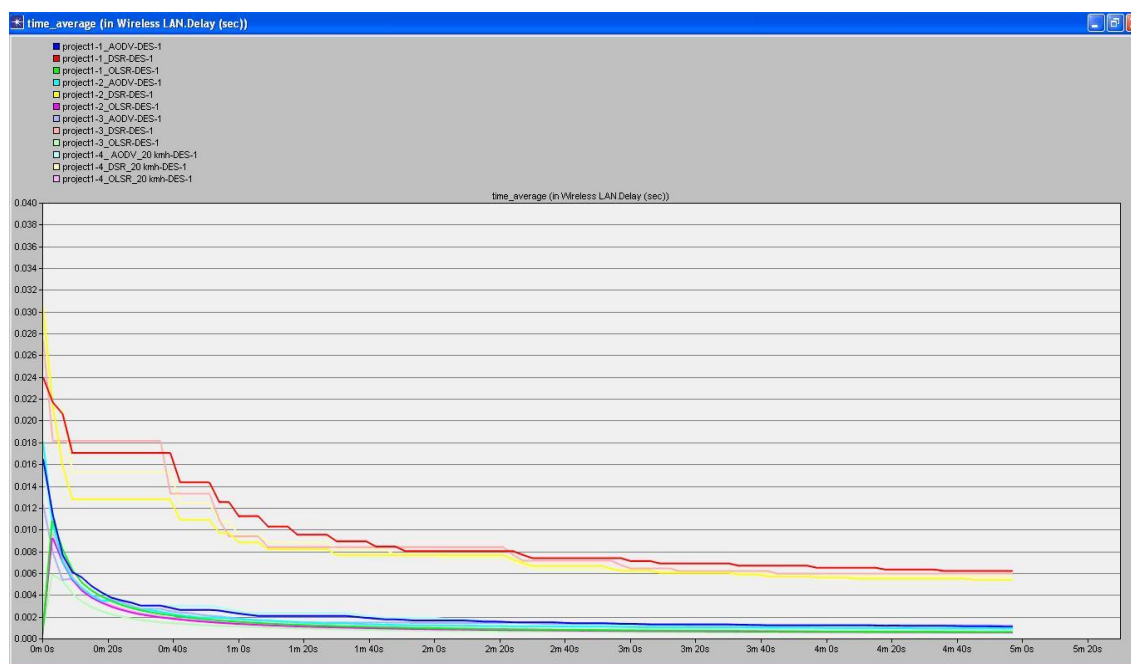
شکل ۵-۵ نتایج بار شبکه در محیط ۴ - AODV, DSR, OLSR

در شکل زیر توان شبکه مورد بررسی قرار گرفته که عملکرد بهتر پروتکل OLSR را نشان می دهد ، همچنین پروتکل DSR عملکرد پایین تری دارد . پروتکل AODV نیز نسبت به DSR توان بهتری دارد .



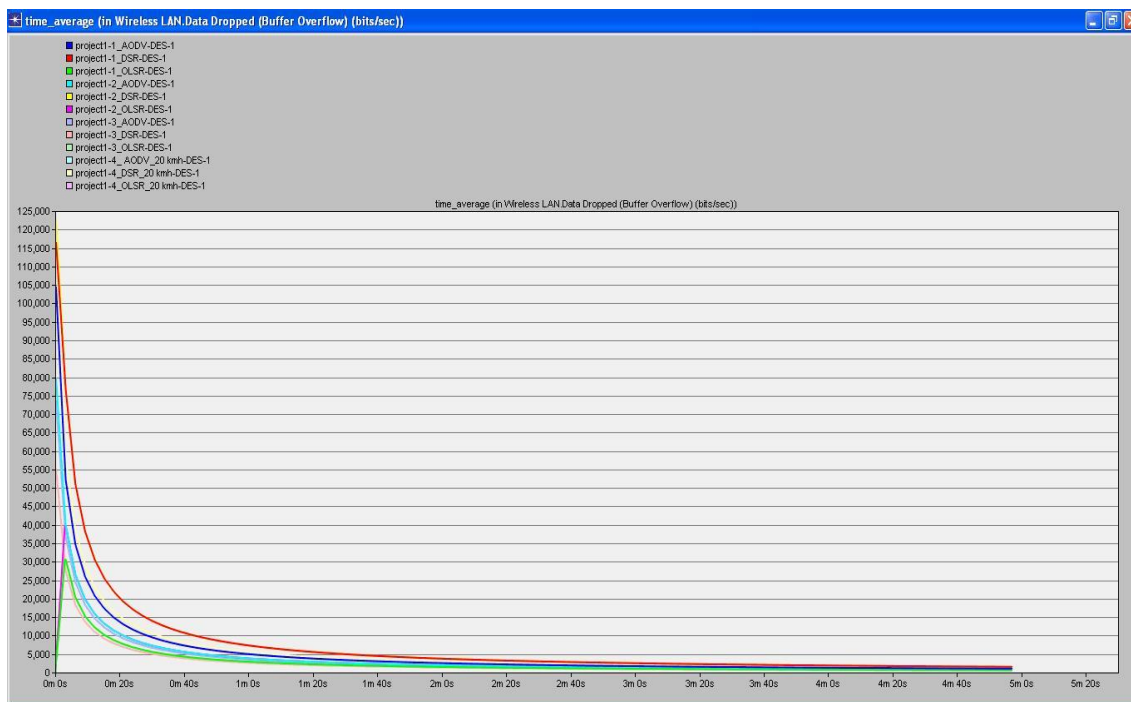
شکل ۵-۵ نتایج توان شبکه در محیط ۴ - AODV, DSR, OLSR

در شکل زیر میزان تاخیر در هر ۴ محیط بر اساس هر ۳ پروتکل را مشاهده می نمایید . با توجه به نمودار نتایج زیر ، پروتکل DSR دارای بیشترین زمان تاخیر می باشد و پروتکل OLSR تاخیر کمتری دارد . پروتکل AODV نیز نسبت به DSR تاخیر کمتری داشته است . البته اگر جزئی تر بخواهیم بررسی کنیم ، پروتکل DSR در محیط اول بیشترین تاخیر و پروتکل OLSR در محیط اول کمترین تاخیر نسبت به بقیه را داشتند .



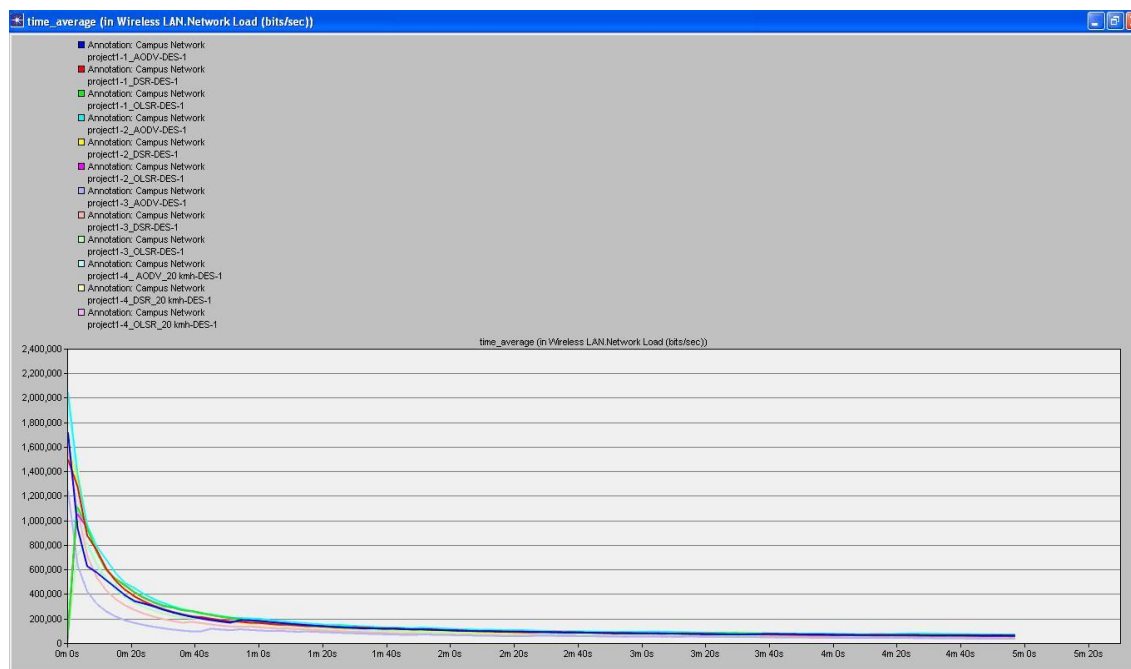
شکل ۵-۲ نتایج میزان تاخیر در ۱۲ سناریو ( همه تاخیر زمان ها )-AODV, DSR, OLSR

در شکل زیر میزان سربار شبکه در هر ۴ محیط بر اساس هر ۳ پروتکل را مشاهده می نمایید . با بررسی این نتایج ، از لحاظ کلی اگر بخواهیم نظر دهیم از لحاظ میزان سربار شبکه ، پروتکل OLSR سربار کمتری دارد و پروتکل DSR سربار بیشتری دارد . در حالت جزئی تر DSR در محیط سوم میزان سربار کمتری داشته و در محیط اول و دوم میزان سربار بیشتری داشته است . البته OLSR در سه محیط دارای کمترین مقدار میزان سربار می باشد . DSR نیز در سه محیط دارای بیشترین میزان سربار بوده است . AODV نیز در این میان نسبت به DSR سربار کمتری داشته و نسبت به OLSR میزان سربار تقریباً بیشتری داشته است .



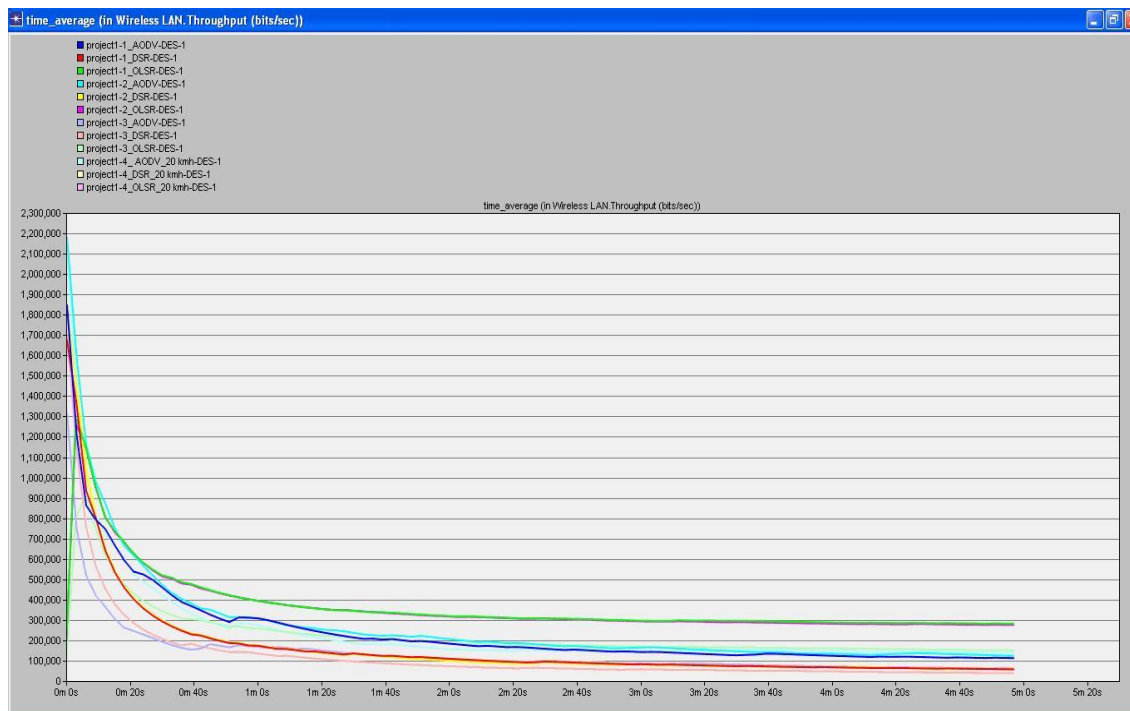
شکل ۵-۳ نتایج میزان سربار شبکه در ۱۲ سناریو ( همه میزان سربارها) -AODV,DSR,OLSR

در شکل زیر بار شبکه در هر ۴ محیط بر اساس هر ۳ پروتکل را مشاهده می نمایید . با بررسی نتایج نمودار زیر ، AODV در محیط دوم دارای بیشترین بار شبکه بوده است . و DSR در محیط سوم دارای کمترین بار شبکه بوده است . DSR در هر چهار محیط دارای کمترین بار شبکه بوده است . در سه محیط نیز OLSR دارای بیشترین بار شبکه بوده است .



شکل ۵-۴ نتایج بار شبکه در ۱۲ سناریو ( همه نتایج در یک نمودار) -AODV,DSR,OLSR

در شکل زیر توان شبکه در هر ۴ محیط بر اساس هر سه پروتکل را مشاهده می نمایید. با بررسی نتایج این نمودار مشخص می شود که OLSR در محیط اول بالاترین مقدار توان را داشته و DSR در محیط سوم دارای کم ترین مقدار توان بوده است. در هر چهار محیط پروتکل OLSR دارای بیشترین مقدار توان بوده و در هر چهار محیط نیز پروتکل DSR دارای کمترین مقدار توان بوده است. پروتکل AODV نسبت به پروتکل DSR نیز دارای مقدار توان بیشتری می باشد.



شکل ۵-۵ نتایج توان شبکه در ۱۲ سناریو ( همه نتایج در یک نمودار) -AODV, DSR, OLSR

## ۵-۶-۵ شبیه سازی دو محیط دیگر با ارائه نتایج

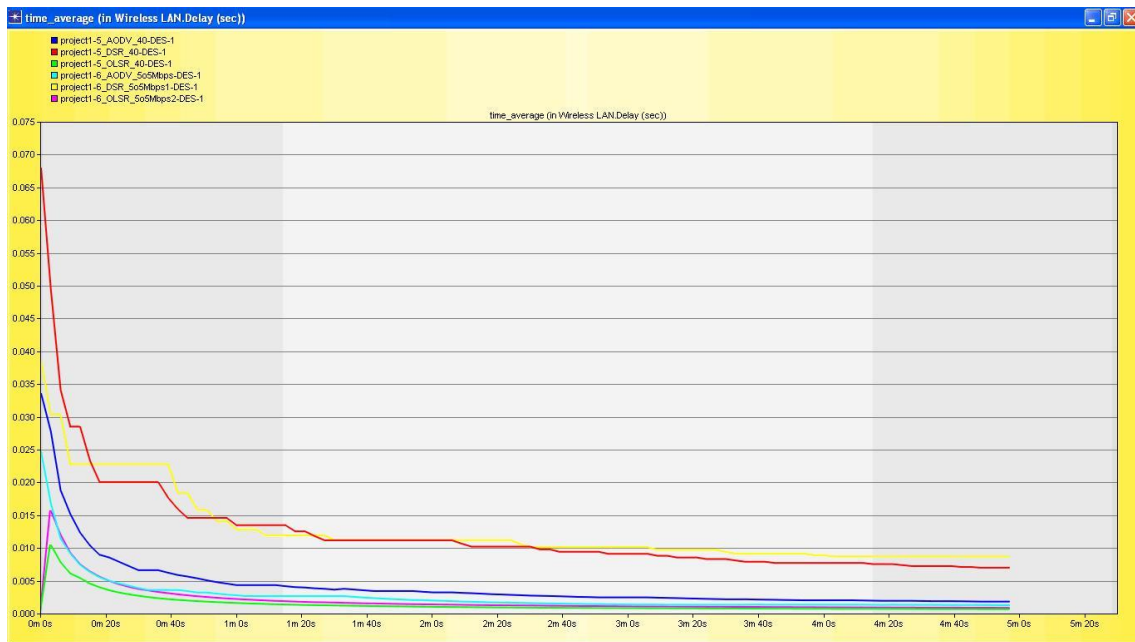
به غیر از چهار محیط بالا در اینجا دو محیط دیگر به شرح ذیل در نرم افزار شبیه سازی، ایجاد نموده و نتایج آن ها را طبق نمودارهای زیر می توانید مشاهده نمایید.

۱ - محیط پنجم دارای ۴۰ نود متحرک موبایل می باشد. بقیه پارامترهای آن نیز مانند محیط اول می باشد.

۲ - محیط ششم نیز دارای نرخ ارسال داده ۵.۵ Mbps می باشد و بقیه پارامترهای آن نیز مانند محیط اول.

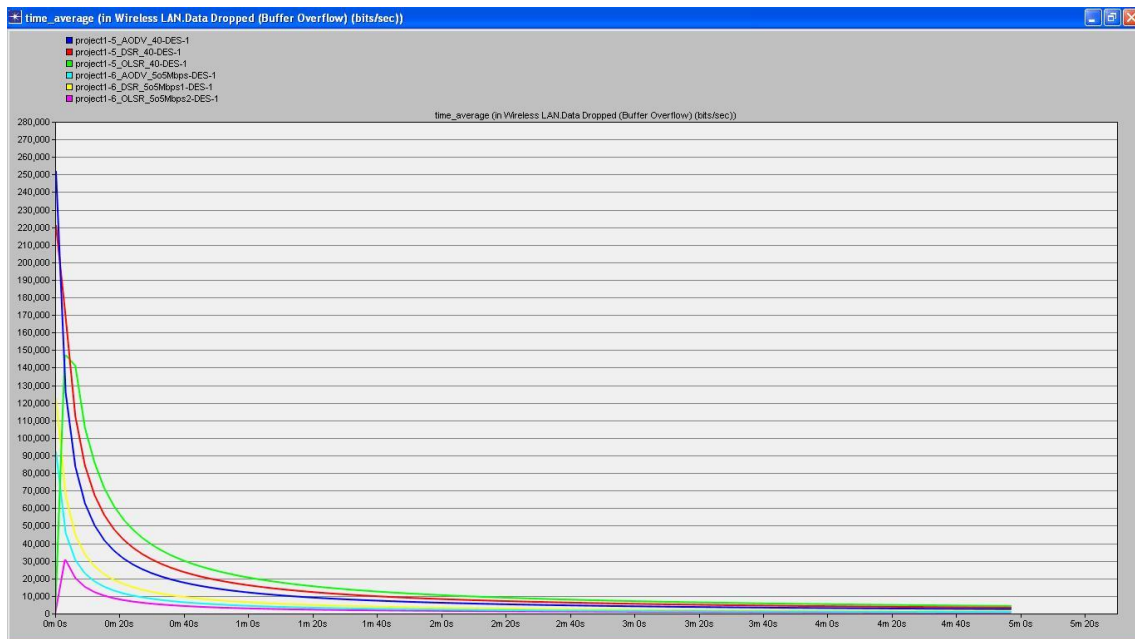
در شکل زیر محیط پنجم و ششم با هر سه پروتکل با معیار تاخیر زمان بررسی شده اند که طبق نتایج زیر DSR نیز دارای بیشترین تاخیر می باشد و OLSR نیز دارای کمترین تاخیر است. AODV نیز نسبت به DSR تاخیر کمتری دارد. در نمودار زیر مشهود است که تاخیر پروتکل DSR محیط ششم با توجه به نرخ ارسال داده کم تر به مرور بیشتر از پروتکل DSR محیط پنجم می شود.





شکل ۵-۶ نتایج میزان تاخیر شبکه در محیط ۶۰۵ – AODV, DSR, OLSR

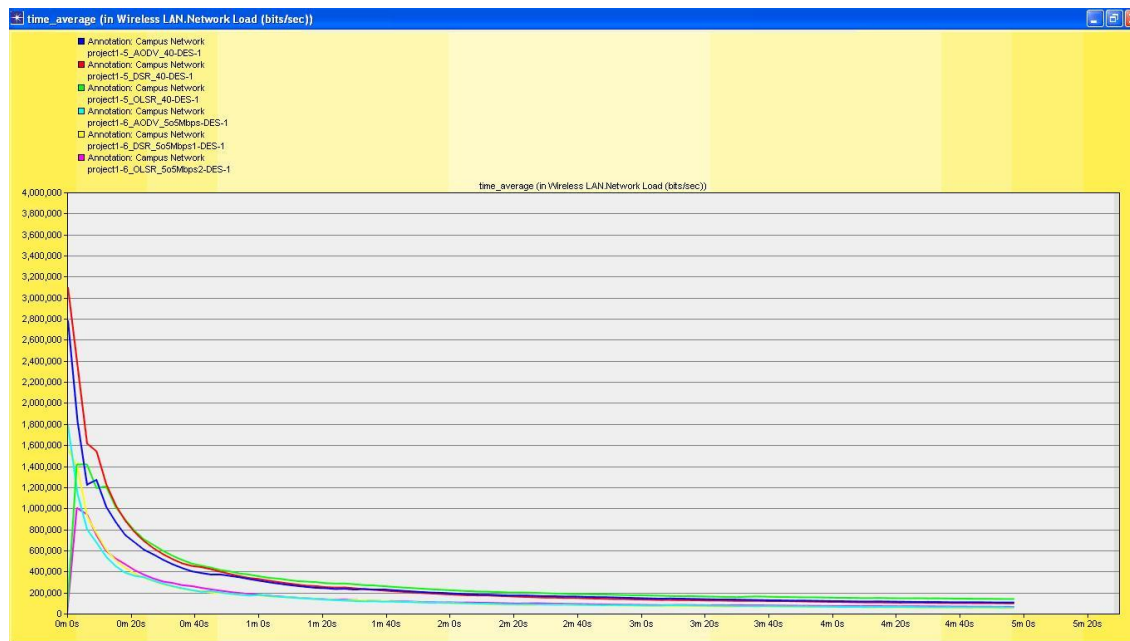
در شکل زیر محیط پنجم و ششم با هر سه پروتکل با معیار میزان سربار شبکه بررسی شده اند که نتایج به این گونه می باشد، پروتکل OLSR در محیط پنجم دارای بیشترین میزان سربار و پروتکل OLSR در محیط ششم دارای کم ترین میزان سربار می باشد. در محیط پنجم OLSR بیشترین سربار شبکه و AODV کمترین سربار شبکه را دارد. در محیط ششم DSR بیشترین سربار شبکه و OLSR کمترین سربار شبکه را دارد. نسبت به DSR نیز در هر دو محیط میزان سربار کم تری در شبکه دارد.



شکل ۵-۷ نتایج میزان سربار شبکه در محیط ۶۰۵ – AODV, DSR, OLSR

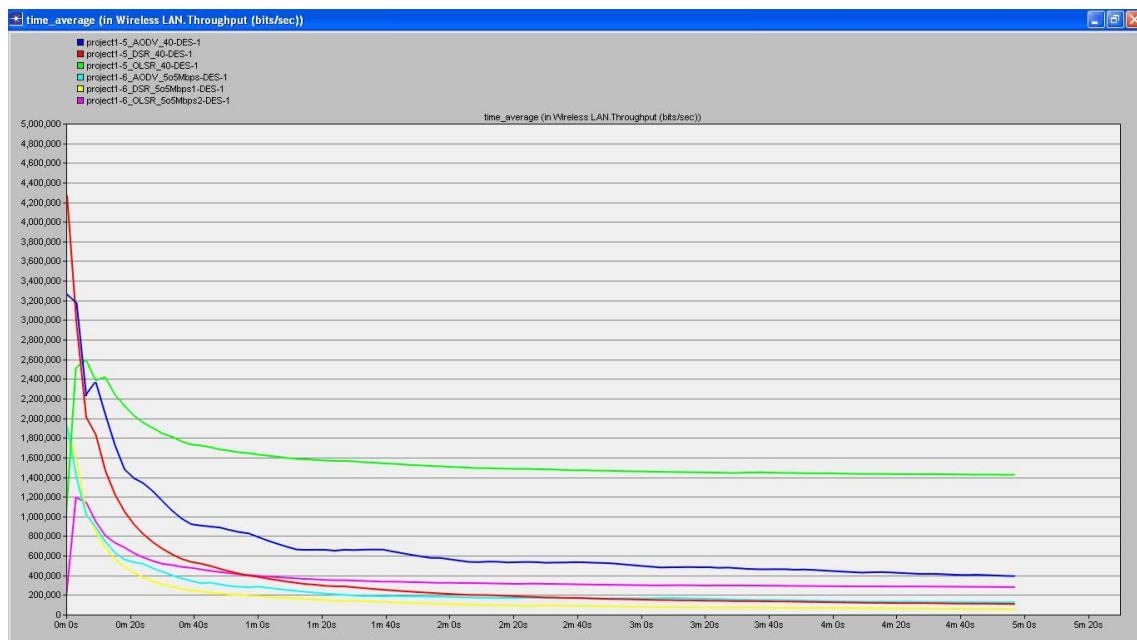


در شکل زیر محیط پنجم و ششم با هر سه پروتکل با معیار بار شبکه بررسی شده اند که طبق نتایج زیر پروتکل OLSR محیط پنجم دارای بیشترین بار شبکه و پروتکل DSR محیط ششم دارای کمترین بار شبکه می باشد. در محیط پنجم، پروتکل OLSR دارای بیشترین بار شبکه و پروتکل DSR نیز کمترین بار شبکه را دارند. در محیط ششم، OLSR دارای بیشترین بار شبکه و DSR نیز کمترین بار شبکه را دارد. در اینجا AODV نسبت به DSR در هر دو محیط بار شبکه بیشتری دارد.



شکل ۵-۵۸ نتایج بار شبکه در محیط ۶۵ - AODV, DSR, OLSR

در شکل زیر محیط پنجم و ششم با هر سه پروتکل با معیار توان شبکه بررسی شده اند که نتایج آن به این گونه می باشد که پروتکل OLSR محیط پنجم دارای بیشترین مقدار توان شبکه و پروتکل DSR محیط ششم دارای کمترین مقدار توان شبکه می باشد. در محیط پنجم و ششم OLSR دارای بیشترین توان و پروتکل DSR دارای کمترین مقدار توان می باشد. در هر دو محیط پروتکل AODV به نسبت DSR نیز توان بالاتری دارد.



شکل ۵-۵۹ نتایج توان شبکه در محیط ۶۰۵ – AODV, DSR, OLSR

جدول ۵-۱ نتایج آماری کل شبیه سازی در ۶ محیط

محیط	پارامتر	AODV			DSR			OLSR		
		ماکزیمم	مینیمم	انحراف معیار	ماکزیمم	مینیمم	انحراف معیار	ماکزیمم	مینیمم	انحراف معیار
۱	Delay (sec)	۰.۰۱۶	۰.۰۰۱۰	۰.۰۰۲۰۳	۰.۰۲۴	۰.۰۰۶۲	۰.۰۰۴۰۶	۰.۰۱۰۸	۰.۰۰۰۶	۰.۰۰۱۵۲
۲		۰.۰۱۸	۰.۰۰۰۹	۰.۰۰۲۱۱	۰.۰۰۳	۰.۰۰۵۳	۰.۰۰۳۵۶	۰.۰۰۹۲	۰.۰۰۰۵	۰.۰۰۱۲۹
۳		۰.۰۱۲	۰.۰۰۱۱	۰.۰۰۱۴۸	۰.۰۲۷	۰.۰۰۵۹	۰.۰۰۴۲۷	۰.۰۰۵۸	۰.۰۰۰۵	۰.۰۰۰۸۹
۴		۰.۰۱۵	۰.۰۰۰۸	۰.۰۰۱۹۴	۰.۰۲۹۷	۰.۰۰۵۷	۰.۰۰۴۱۰	۰.۰۰۹۶	۰.۰۰۰۵	۰.۰۰۱۳۶
۵		۰.۰۳۳	۰.۰۰۱۸	۰.۰۰۴۶۷	۰.۰۶۸	۰.۰۰۶۹	۰.۰۰۸۴۰	۰.۰۱۰۵	۰.۰۰۰۶	۰.۰۰۱۴۹
۶		۰.۰۲۴۷	۰.۰۰۱۲	۰.۰۰۳۱۱	۰.۰۳۸۶	۰.۰۰۸۷	۰.۰۰۵۶۰	۰.۰۱۵۷	۰.۰۰۰۸۷	۰.۰۰۲۲۳
۱	Buffer Overflow (bit/s)	۱۰۴۴۴۸	۱۰۴۴	۱۲۲۰۶	۱۱۶۷۳۶	۱۵۳۶	۱۵۱۱۰	۳۰۷۲۰	۶۱۴	۴۱۶۵
۲		۷۹۸۷۲	۷۹۸	۹۳۳۴	۱۲۲۸۸۰	۱۵۳۶	۱۵۵۶۰	۳۹۹۳۶	۷۹۸	۵۴۱۵
۳		۷۳۷۲۸	۷۳۷	۸۶۱۶	۵۵۲۹۶	۵۵۲	۶۴۶۲	۳۹۹۳۶	۷۹۸	۵۴۱۵
۴		۷۳۷۲۸	۷۳۷	۸۶۱۶	۱۱۶۷۳۶	۱۱۶۷	۱۳۶۴۳	۳۰۷۲۰	۶۱۴	۴۱۶۵
۵		۲۵۱۹۰۴	۲۵۱۹	۲۹۴۴۰	۲۲۱۱۸۴	۳۳۷۹	۳۰۷۶۶	۱۴۷۴۵۶	۴۳۰۰	۲۴۹۲۴
۶		۹۲۱۶۰	۹۲۱	۱۰۷۷۰	۱۲۲۸۸۰	۱۳۵۱	۱۴۸۱۷	۳۰۷۲۰	۶۱۴	۴۱۶۵
۱	Network Load (bit/s)	۱۷۱۷۲۴۸	۶۱۷۲۵	۲۰۶۱۹۴	۱۴۹۸۶۶۶	۵۵۶۰۱	۲۲۲۱۸۷	۱۱۱۰۸۵۳	۶۵۸۴۷	۱۷۱۲۹۰
۲		۲۰۴۴۷۵۷	۶۹۹۵۴	۲۶۷۸۳۰	۱۶۰۶۴۳۲	۵۵۳۵۳	۲۳۴۰۸۱	۱۰۵۵۰۱۳	۶۱۸۱۶	۱۶۹۲۶۴
۳		۱۲۴۷۳۳۸	۳۸۵۴۱	۱۴۰۶۰۱	۱۵۹۲۳۷۳	۳۶۹۴۶	۲۰۴۶۶۶	۸۱۹۷۶۸	۴۸۶۵۶	۱۳۵۱۵۰
۴		۱۹۹۵۶۹۰	۶۴۷۳۳	۲۴۳۵۳۰	۱۵۰۱۰۱۳	۵۵۵۲۸	۲۳۳۸۹۹	۱۰۷۶۵۸۶	۶۸۷۴۷	۱۶۸۹۷۵
۵		۲۷۸۷۹۸۹	۱۰۵۲۲۵	۳۶۷۳۳۰	۳۰۹۹۱۱۴	۹۶۸۶۸	۴۴۴۰۴۶	۱۴۱۷۶۵۳	۱۳۸۸۷۱	۲۶۴۵۸۷
۶		۱۷۹۰۹۹۷	۵۸۴۴۶	۲۲۸۳۰۹	۱۵۶۶۱۷۶	۵۱۵۱۷	۲۳۴۹۸۹	۱۰۰۲۳۳۰	۶۳۱۳۱	۱۶۵۲۹۱

۱	Throughput (bit/s)	۱۸۵۱۴۴۵	۱۱۲۲۴۷	۲۴۲۶۲۷	۱۶۷۶۶۱۸	۵۷۲۷۴	۲۴۱۵۵۶	۱۲۸۹۰۳۴	۲۸۲۱۴۲	۱۶۸۳۶۱
۲		۲۱۸۱۸۰۲	۱۲۳۵۱۹	۲۹۵۵۶۸	۱۸۲۸۵۵۴	۵۷۵۷۴	۲۵۹۰۹۹	۱۲۵۹۵۱۴	۲۷۵۷۵۵	۱۶۷۲۹۶
۳		۱۳۲۰۴۴۸	۶۱۹۵۲	۱۵۳۲۶۸	۱۷۰۷۱۳۶	۳۸۰۹۴	۲۱۷۹۳۸	۹۱۰۰۸۰	۱۵۰۴۸۳	۱۳۳۲۳۰
۴		۲۱۲۹۷۸۱	۱۳۹۷۱۱	۲۶۹۶۹۴	۱۷۷۱۲۹۶	۵۸۲۳۰	۲۶۳۸۷۰	۱۲۶۷۴۵۶	۲۷۹۲۵۸	۱۶۷۸۵۷
۵		۳۲۶۳۸۹۳	۳۹۲۱۴۲	۵۱۴۳۹۹	۴۲۶۸۳۴۱	۱۰۸۶۱۱	۵۷۷۱۹۳	۲۵۹۳۳۹۷	۱۴۲۴۶۹۲	۲۴۵۲۹۸
۶		۱۹۲۴۰۳۲	۱۲۶۱۵۱	۲۵۵۹۸۷	۱۹۱۹۱۴۶	۵۵۰۴۷	۲۷۴۵۶۱	۱۱۹۱۳۳۸	۲۸۰۴۶۸	۱۶۲۴۳۰

## ۵-۷ جمع بندی

در ابتدای کار باید این نکته را عرض کنم که این شبیه سازی بر اساس یک شرایط و پارامترهایی انجام شده است و نتایج آن بدست آمد. بنابراین ممکن است در شرایط دیگری با پارامترهای مختلف، نتایج متفاوتی بدست آید. با توجه به نتایج بدست آمده طبق شکل های بالا، عملکرد پروتکل OLSR نسبت به AODV و DSR بهتر می باشد. در نتایج شبیه سازی با توجه به پارامتر تاخیر زمان، پروتکل OLSR دارای کمترین تاخیر و پروتکل DSR بیشترین تاخیر را دارد. از لحاظ میزان سربار نیز در شرایط مختلف شبکه فرق می کند و به طور صریح نمی توان گفت که کدام بهتر عمل می کند. در چهار محیط OLSR سربار کمتر و DSR سربار بیشتری داشته است. همچنین در چهار محیط AODV نسبت به DSR سربار کمتری داشته است. مثلاً در محیط اول DSR سربار بیشتر و OLSR سربار کمتری داشته ولی در محیط پنجم که نودها دو برابر شده اند، OLSR سربار بیشتری داشته و AODV سربار کمتری داشته است. در محیط سوم که نودهای متحرک کمتر از بقیه بودند، OLSR سربار بیشتر و DSR سربار کمتر داشته، البته نتایج خیلی نزدیک به هم بوده اند. در هر صورت به طور میانگین پروتکل OLSR دارای سربار کمتر و DSR دارای سربار بیشتری بوده است. اگر بخواهیم از نظر میزان سربار بین دو پروتکل AODV و DSR نظر دهیم، با توجه به نتایج، پروتکل AODV در مجموع میزان سربار کمتری دارد. از لحاظ بار شبکه نیز با توجه به نتایج، غیر از محیط دوم، در بقیه محیط ها پروتکل OLSR دارای بار شبکه بیشتری بوده و در همه محیط ها پروتکل DSR دارای میزان بار شبکه کمتری بوده است. در مورد مقایسه بین پروتکل های AODV و DSR در همه محیط ها با توجه به نمودارهای نتایج، پروتکل AODV بار شبکه بیشتری داشته است. از نظر پارامتر توان شبکه نیز در همه حالت ها پروتکل OLSR دارای بیشترین مقدار توان شبکه می باشد و پروتکل DSR دارای کمترین مقدار توان شبکه است. در مقایسه بین دو پروتکل AODV و DSR نیز مقدار توان شبکه پروتکل AODV بالاتر می باشد.

## فصل ششم

### جمع بندی و ارائه پیشنهادات

## ۶-۱ جمع بندی و ارائه پیشنهادات

در ابتدا لازم می دانم این نکته را ذکر کنم که نتایج این شبیه سازی بر اساس یک شرایطی بوده است و ممکن است در شرایط دیگری، نتایج فرق داشته باشد. این نوشتار به طور کلی شامل دو مطالعه، یکی بررسی تحلیلی شبکه های اقتضائی متحرک و پروتکل های مسیریابی در آن و دیگری بحث شبیه سازی سه نوع پروتکل مسیریابی بوده است. در قسمت تحلیلی به این نتیجه رسیدیم که در دنیای مدرن ارتباطات از راه دور امروزه، پروتکل های مسیریابی نقش برجسته و مهمی را در شبکه ها برعهده دارند. پروتکل های مسیریابی هر کدام بر اساس ویژگی ها و خصوصیات خاص خود، مخصوص شرایط و مقتضیات مکان خود می باشند. بر این اساس انتخاب پروتکل مناسب با توجه به شبکه، قطعا قابلیت اطمینان از این شبکه را بالا می برد. با توجه به نتایج بدست آمده می توان گفت الگوریتمی برای مسیریابی شبکه های اقتضائی متحرک مناسب است که عملکرد مناسبی در محیط های پرتحرک داشته و همچنین دارای تاخیر و سربار کمی باشد و بتواند بهینه ترین مسیر را پیدا کند. البته امنیت در شبکه های اقتضائی از وضعیت ویژه ای برخوردار است. زیرا در این شبکه ها علاوه بر تمامی مشکلات موجود در شبکه های با سیم، با مشکلات امنیتی همچون سادگی شنود و تغییر اطلاعات در حال انتقال، امکان جعل هویت افراد، شرکت نکردن و یا تخریب عملیات مسیریابی، عدم امکان استفاده از زیرساختهای توزیع کلید رمزنگاری و غیره مواجه می شویم. بنابراین با توجه به موارد بالا، باید به دنبال یک پروتکل مسیریابی امن در شبکه های اقتضائی بود. یکی از دسته بندی های معمول پروتکل های مسیریابی، روشهای فعال \_ کنش گرا (برحسب جدول) و واکنشی (برحسب تقاضا) می باشد. در پروتکل های مبتنی بر جدول، نودها به طور متناوب و در بازه های زمانی مشخص وجود مسیر بین خود تا نودهای دیگر را بررسی کرده و نسبت به نگهداری مسیرهای معتبر و به روز تلاش می کنند. در مقابل پروتکل های برحسب تقاضا، مسیرها فقط در صورت لزوم کشف می شوند. یعنی کشف مسیر زمانی صورت می گیرد که ترافیک داده جهت ارسال وجود داشته باشد. پروتکل های مبتنی بر جدول به علت ایجاد سرباره زیاد در شرایط تحرک زیاد نودها، استفاده غیر معمول از منابع شبکه جهت نگهداری اطلاعات بلااستفاده برای شبکه های اقتضائی شلوغ با تحرک زیاد چندان مناسب نیست. مشکلات پروتکل های مبتنی بر جدول این است که نگهداری و بهنگام سازی جداول مسیریابی به پهنای باند زیادی نیاز دارد و همچنین خیلی از اطلاعات مسیریابی هرگز استفاده نمی شوند، در نتیجه منابع تلف می گردند. مشکلات پروتکل های مبتنی بر تقاضا، تاخیر قبل از فرستادن اولین بسته و همچنین پخش سل آسا برای کشف مسیر می باشد. همچنین مقیاس پذیری بسیاری از پروتکل های مسیریابی مبتنی بر تقاضا به خاطر افزایش جمعیت

و حرکت نودها محدود است. در قسمت شبیه سازی به بررسی سه پروتکل مسیریابی در شبکه های اقتضائی متحرک پرداخته و عملکرد آن ها را بر اساس پارامترهایی مورد ارزیابی قرار دادیم. در اینجا پروتکل های مسیریابی مورد بحث از دو نوع مختلف می باشند. پروتکل های مسیریابی AODV و DSR از نوع واکنشی (بر حسب تقاضا) هستند و پروتکل OLSR از نوع کنش گرا یا مبتنی بر جدول می باشد. طبق نتایج شبیه سازی که بدست آمد، به طور میانگین می توان عملکرد پروتکل OLSR را بهتر دانست. از نظر تاخیر زمان دارای کمترین تاخیر و از نظر توان شبکه نیز دارای مقدار بالایی بود. از نظر میزان سربار شبکه نیز در چهار محیط مقدار کمتری داشته و از لحاظ بار شبکه نیز دارای مقدار بیشتری بود. در پروتکل OLSR مهمترین مکانیزم، انتخاب گره های ارسال چند نقطه ای می باشد که این گره ها اطلاعات کنترلی را در شبکه پخش و مسیریابی از طریق این گره ها انجام می شود. برای بهبود این پروتکل می توان از الگوریتم هایی استفاده نمود تا پروتکل OLSR از کیفیت خدمات سرویس<sup>1</sup> پشتیبانی نماید. (یعنی الگوریتم های جدیدی برای انتخاب گره های ارسال چند نقطه ای). با توجه به این که پروتکل OLSR تنها از نظر تعداد گام بهینه است (کوتاهترین مسیر ممکن)، معیارهای کیفیت خدمات سرویس (تاخیر و پهنای باند) برای مسیریابی مهیا می شود<sup>2</sup>. در این صورت زمان ارسال بسته ها و همچنین نرخ از دست رفتن آن ها بهبود می یابد. DSR به علت تاخیر زیاد و تعداد اندک بسته های داده موفق در شرایط شلوغی شبکه و تحرک زیاد گره ها، چندان مناسب نیست. AODV به علت سادگی و نیاز محدود به منابع شبکه، حجم پردازش کم و تاخیر مسیریابی نسبتاً قابل قبول، انتخاب خوبی است. این پروتکل به علت معیار مسیریابی خود که سرعت مسیر می باشد، کمتر با ازدحام مسیرها روبه رو خواهد شد و در شرایط شلوغی شبکه (محیط پنجم) در مقایسه با پروتکل DSR از تاخیر ارسال داده کمتر و تعداد بسته داده موفق بیشتری برخوردار می باشد. لیکن با توجه به این نکته که هرچند پروتکل AODV با استقبال خوبی مواجه شده ولی با مشکلات سرباره مسیریابی زیاد و همچنین تاخیر ارسال داده زیاد در هنگام شکست پیوندها رو به رو می باشد. بنابراین با اصلاح و ارائه روش های جدید می توان در جهت بهبود این پروتکل ها گام برداشت. با توجه به این که پروتکل AODV از معیار کمترین تعداد گام استفاده می کند می توان برای افزایش کارائی الگوریتم مسیریابی AODV از منطق فازی استفاده نمود. ورودی سیستم فازی، ترکیب اطلاعات مربوط به ازدحام گره با تعداد گام ها می باشد. الگوریتم اصلاح شده FAODV می باشد. شناسایی وضعیت تراکم گره، شناسایی سطح تراکم مسیر و مسیریابی با استفاده از منطق فازی از جزئیات این الگوریتم اصلاح شده است. همچنین در

1 - QOS

2 - QOLSR

سالهای اخیر با توجه به کاربردهای حساس شبکه های اقتضائی از جمله در عملیاتهای نظامی، فوریتهای پزشکی و یا مجامع و کنفرانسها، که نیاز به تامین امنیت در این شبکه ها بارزتر شده است، محققان برای تامین امنیت در دو حیطه عملکرد و اعتبار پیشنهادات گوناگونی را مطرح کردند و می کنند . از این میان می توان به پروتکل های SEAD<sup>۱</sup>, Ariadne<sup>۲</sup>, SRP<sup>۳</sup>, SAODV<sup>۴</sup>, ARAN<sup>۵</sup>, SPAAR<sup>۶</sup> و غیره اشاره کرد.

از جمله مسائلی قابل بحث در آینده بر روی شبکه های اقتضادی می توان به موارد زیر اشاره نمود :

- ۱) بدست آوردن مدلی برای مشکلات امنیتی مسیریابی امن
- ۲) ارزیابی و مقایسه علمی بین انواع پروتکل های جدید
- ۳) روشهای استاندارد برای بررسی و طراحی امن شبکه های اقتضائی متحرک
- ۴) طراحی بهینه پروتکل مسیریابی با توجه به بده-بستان بین امنیت و عملکرد
- ۵) ارائه پیشنهادات برای اصلاح پروتکل های مسیریابی شبکه های اقتضائی متحرک
- ۶) طراحی و ارائه پروتکل مسیریابی مطمئن و با کارکرد بالا برای شبکه های اقتضائی متحرک
- ۷) شبیه سازی پروتکل های مسیریابی در نرم افزارهای شبیه ساز برای آنالیز عملکرد آن ها در جهت پیاده سازی آن ها در محیط واقعی

- 
- 1- Secure Efficient Ad hoc Distance Routing Protocol
  - 2- Secure Routing Protocol
  - 3- Secure AODV
  - 4-Authenticated Routing for Ad hoc Networks
  - 5- Secure Position Aided Ad-hoc Routing Protocol

## پیوست الف

### آموزش نرم افزار شبیه سازی OPNET

( Optimized Network Engineering Tool )

( OPTimum Network performance )



## الف- ۱ مقدمه

شبیه ساز OPNET که در دانشگاه MIT و در سال ۱۹۸۷ ارائه شد این امکان را برای کاربر فراهم می کند تا به طراحی و مطالعه شبکه های مخابراتی، ادوات شبکه و پروتکل های موجود در شبکه بپردازد. یکی از قابلیت های این شبیه سازی گرا بودن آن است از قابلیت های دیگر آن سلسله مراتبی بودن روند طرح ریزی مسائل می باشد. OPNET یک شبیه ساز تجاری است که برای شبیه سازی پروتکل های رایج در شبکه و مدل های مختلف در شبکه های با رنج بسیار متنوع به کار می رود. این نرم افزار بر روی سیستم عامل های Windows و Solaris قابل نصب می باشد.

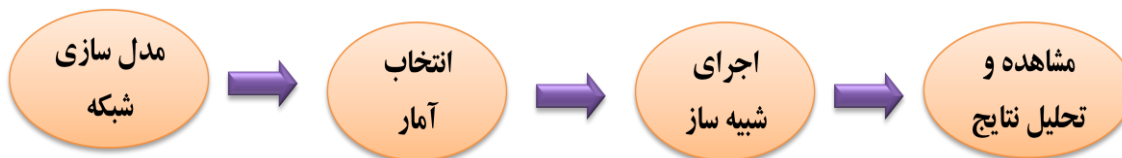
## الف- ۲ کاربردهای مهم OPNET

- آنالیز شبکه های فعلی از طریق شبیه سازی: این نرم افزار مستقیماً می تواند فایل های تنظیمات (Configuration) روترهای سازندگان مختلف مانند سیسکو را به عنوان ورودی دریافت کرده و سناریوی فعلی شبکه را شبیه سازی کند.
  - طراحی بهینه شبکه: با این نرم افزار می توان لینک ها را به صورت بهینه انتخاب کرد تا از هزینه های اضافی جلوگیری شود.
  - شبیه سازی عملکرد پروتکل های جدید که در محیط های تحقیقاتی به وجود آمده اند. ایجاد این پروتکل ها بر اساس برنامه نویسی C++ و ماشین حالت منتهای (FSM) می باشد.
- با توجه به کتابخانه بزرگ این نرم افزار که شامل انواع روترها، سویچ و سایر تجهیزات سازندگان بزرگی مانند سیسکو، Com3، ژونپیر و غیره است، جز در مواردی محدود نیازی به استفاده از ویرایشگرهای گره و پروسه نیست و تنها از طریق ویرایشگر اصلی که ویرایشگر شبکه نامیده می شود می توان شبکه را پیاده سازی کرد و نتایج شبیه سازی عملکرد آن را به صورت نمودارهای مختلف مشاهده نمود.
- OPNET در ارائه نتایج نیز بسیار کارآمد است. این نرم افزار می تواند نتایج شبیه سازی را علاوه بر نمایش به صورت گراف های متعدد، به صورت صفحه وب نیز ارائه کند.
- قابلیت بسیار جالب OPNET امکان وارد کردن فایل های تنظیمات روترها و سویچ ها شبکه فعلی در نرم افزار است. فناوری های بی سیم در سال های اخیر در کشورمان گسترش فراوانی یافته اند. این فناوریها در شبکه های محلی بی سیم، لینک های نقطه به نقطه و لینک های نقطه به چند نقطه مورد استفاده ISP ها، شرکت های تجاری و شرکت های دولتی قرار می گیرند. نرم افزارهای مختلفی را می توان برای شبیه سازی این شبکه ها استفاده کرد. با

این وجود بیشتر این نرم افزارها یا توانایی شبیه سازی و اعمال ترافیک لایه ها بالاتر (TCP/IP) راندارند و یا از قابلیت های لازم برای شبیه سازی تأثیر مدولاسیون ها، پرتوی آنتن ها و محیط انتقال برخوردار نیستند.

### الف-۳ توصیف کاملی از شبیه ساز OPNET

- این شبیه ساز ابزارهای پر قدرتی را در جهت کمک به کاربر در انجام ۴ مرحله مختلف یک شبیه سازی فراهم می کند.

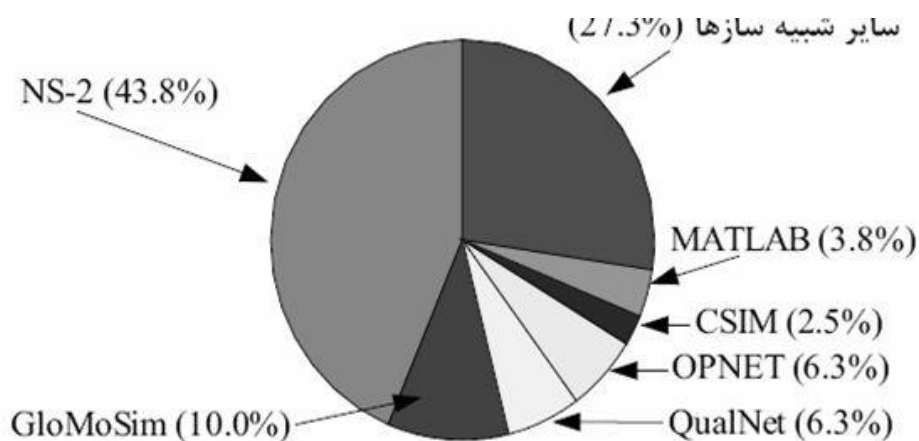


شکل الف-۱ چهار مرحله شبیه سازی توسط نرم افزار opnet

- در شبیه ساز OPNET یک ساختار سلسله مراتبی برای شبیه سازی به کار می رود به عبارت دیگر مساله در سطوح مختلف تعریف می گردد.
- کتابخانه این شبیه ساز بسیار کامل بوده و شامل آخرین پروتکل ها و مدل های ارائه شده در زمینه شبکه می باشد.

### الف-۴ OPNET در مقایسه با سایر شبیه سازها

بر خلاف NS-2 که open source می باشد، OPNET نیاز به خرید لایسنس دارد که بسیار گران است. واسطه گرافیکی OPNET بسیار ساده و جذاب است و برای برنامه نویسی نیاز به آشنایی با زبان C++ , C دارد. گفته میشود این اولین نرم افزار است که برای شبیه سازی شبکه به بازار آمد اما مدتی NS-2 به دلیل open source بودن طرفداران بیشتری پیدا کرد. اما در سالهای اخیر به دلیل رونق شبکه های بی سیم و کارایی بی نظیر OPNET در شبیه سازی شبکه های بی سیم و موبایل (متحرک) دوباره OPNET در صدر قرار گرفت. ضمن اینکه OPNET بسیاری از وظایف را به صورت اتوماتیک انجام می دهد و نیاز به برنامه نویسی هر چیز کوچکی از پایین ترین سطح نیست. از دیگر مزایای OPNET، سرعت اجرای بسیار بالاست. برنامه ای که در NS-2 شاید نیاز به یک روز وقت برای اجرا داشته باشد در OPNET در عرض چند ثانیه شبیه سازی میشود. البته OPNET از لحاظ سرعت هنوز نمی تواند از MATLAB بهتر عمل کند. همچنین این نرم افزار قابلیت ارتباط با MATLAB و استفاده از برنامه های MATLAB جهت مدلسازی در پایتترین سطح (سطح پروسس) را دارد.



شکل الف-۲ میزان استفاده از شبیه سازهای مختلف بمنظور شبیه سازی شبکه های MANET

## الف-۵ نصب OPNET

این نرم افزار دارای چندین ورژن می باشد از جمله ۸، ۱۰، ۱۲، ۱۴ که روش نصب آنها با بالا رفتن ورژن ساده تر شده است.

در مراحل نصب این نرم افزار باید دقت کافی انجام گردد در غیر اینصورت علاقم نصب ساده خود نرم افزار نمی توانید از شبیه سازی خود نتیجه ای دریافت کنید، در زیر مراحل نصب OPNET ورژن ۱۴ را خواهید دید که باید به ترتیب انجام گیرد:

(۱) نصب Visual Studio 2005

(۲) باز کردن Visual Studio 2005

(۳) برای نصب خود نرم افزار سه قسمت وجود دارد که باید به ترتیب هرکدام را نصب کنید که عبارتند از:

☐ modeler\_140A\_PL3\_6313\_win

☐ modeler\_docs\_140A\_PL2\_24-Sep-2007\_win

☐ models\_140A\_PL3\_17Oct07\_win

(۴) بعد از نصب این قسمت ها به قسمت environment variable به آدرس زیر رفته و مسیرهای گفته شده

را برای ارتباط نرم افزار با کامپایلر مربوطه وارد کنید.

☐ Right click to My computer > properties > advanced tab > environment variable

مسیرها:

☐ Variable 1: Path

☐ Value:

☐ C:\Program Files\Microsoft Visual Studio 8\Common7\IDE;

☐ C:\Program Files\Microsoft Visual Studio 8\VC\BIN;

☐ C:\Program Files\Microsoft Visual Studio 8\Common7\Tools;

- ☐ C:\Program Files\Microsoft Visual Studio 8\Common7\Tools\bin;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\PlatformSDK\bin;
- ☐ C:\Program Files\Microsoft Visual Studio 8\SDK\v2.0\bin;
- ☐ C:\WINNT\Microsoft.NET\Framework\v2.0.50727;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\VC Packages;
- ☐ C:\Program Files\Microsoft Visual Studio 8\SDK\v2.0\Bin;
- ☐ C:\WINNT\Microsoft.NET\Framework\v2.0.50727;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\bin;
- ☐ C:\Program Files\Microsoft Visual Studio 8\Common7\IDE;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\vcpackages;
- ☐ Variable 2 : INCLUDE
- ☐ Value:
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\ATLMFC\INCLUDE;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\INCLUDE;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\PlatformSDK\include;
- ☐ C:\Program Files\Microsoft Visual Studio 8\SDK\v2.0\include;
- ☐ Variable 3: LIB
- ☐ Value:
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\ATLMFC\LIB;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\LIB;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\PlatformSDK\lib;
- ☐ C:\Program Files\Microsoft Visual Studio 8\SDK\v2.0\lib;
- ☐ Variable 4: LIBPATH
- ☐ Value:
- ☐ C:\WINNT\Microsoft.NET\Framework\v2.0.50727;
- ☐ C:\Program Files\Microsoft Visual Studio 8\VC\ATLMFC\LIB;
- ☐ Variable 5: NetSamplePath
- ☐ Value: C:\Program Files\Microsoft Visual Studio 8\SDK\v2.0;
- ☐ Variable 6: DevEnvDir
- ☐ Value: C:\Program Files\Microsoft Visual Studio 8\Common7\IDE;
- ☐ Variable 7: FrameworkDir
- ☐ Value: C:\WINNT\Microsoft.NET\Framework;
- ☐ Variable 8: FrameworkSDKDir
- ☐ Value: C:\Program Files\Microsoft Visual Studio 8\SDK\v2.0;
- ☐ Variable 9: FrameworkVersion
- ☐ Value: v2.0.50727;
- ☐ variable 10: VCBUILD\_DEFAULT\_CFG

- ☐ value: Debug^|Win32;
- ☐ Variable 11: VCBUILD\_DEFAULT\_OPTIONS
- ☐ Value: /useenv;
- ☐ Variable 12: VCINSTALLDIR
- ☐ Value: C:\Program Files\Microsoft Visual Studio 8\VC;
- ☐ Variable 13: VSINSTALLDIR
- ☐ Value: C:\Program Files\Microsoft Visual Studio 8;

### توجه :

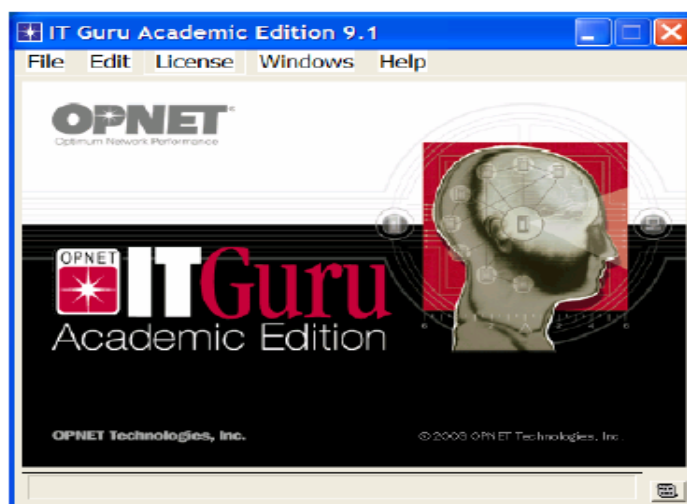
بعد از وارد کردن مسیرها یک Command Prompt باز کرده و به ترتیب دستور cl و سپس link را وارد می کنید.

۵) به شاخه <opnet\_dir>\sys\pc\_intel\_win32\bin\manifest رفته و فایل های موجود در آن را به شاخه <opnet\_dir>\sys\pc\_intel\_win32\bin کپی نمایید.

۶) در نهایت برای کرک کردن نرم افزار کافی است فایل زیر را اجرا نمایید توجه داشته باشید که نرم افزار زیر تجاری بوده و برای اجرای صحیح آن نیاز به خرید نرم افزار دارید لذا مثل سایر نرم افزارهای استفاده شده در ایران برای اجرای صحیح آن از کرک این نرم افزار استفاده می کنیم :

### OPNET.Modeler.14.5.License.Maker-FFS

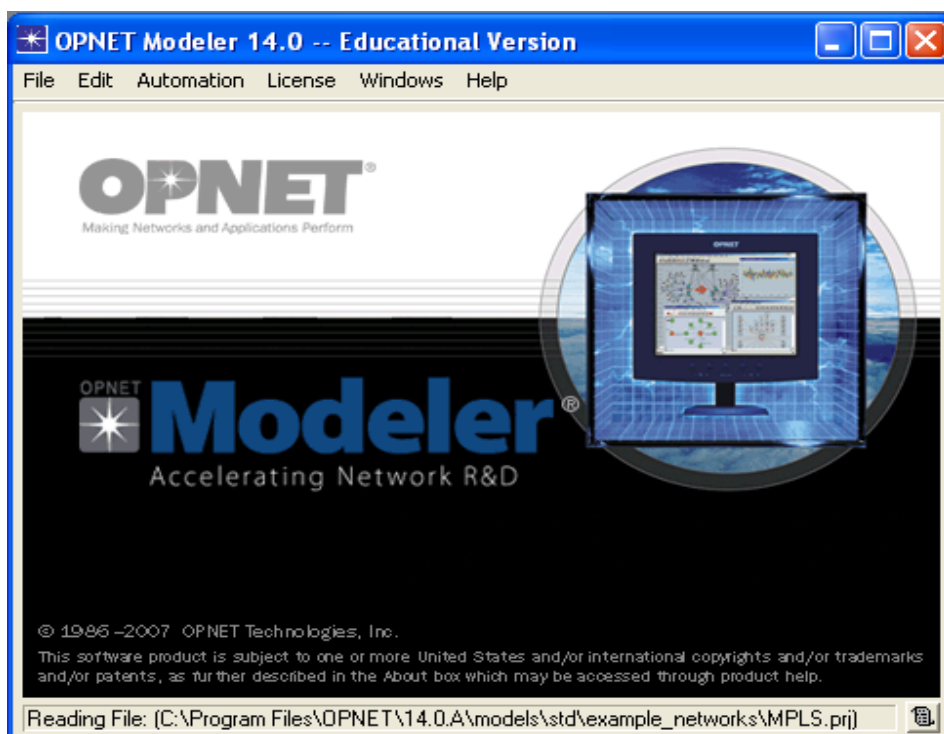
البته با مراجعه به سایت این نرم افزار می توانید فایل آموزشی آن را به رایگان دریافت نمایید منتها این نسخه از نرم افزار فاقد پروتکل ها و مدل ها بوده و برای داشتن آنها نیاز است که خود ، برنامه نویسی آنها را انجام دهید.



شکل الف-۳ نرم افزار رایگان OPNET IT Guru Academic Edition 9.1

بعد از انجام کلیه مراحل با مراجعه به آدرس زیر نرم افزار را اجرا می نمایید :

Start > All programs > OPNET Modeler 14.0 > OPNET Modeler 14.0.exe



شکل الف-۴ پنجره شروع به کار نرم افزار opnet

## الف-۶ ساختار سلسله مراتبی در شبیه ساز OPNET

محیط شبیه سازی دارای سه سطح طراحی می باشد :

☐ Project یا Network

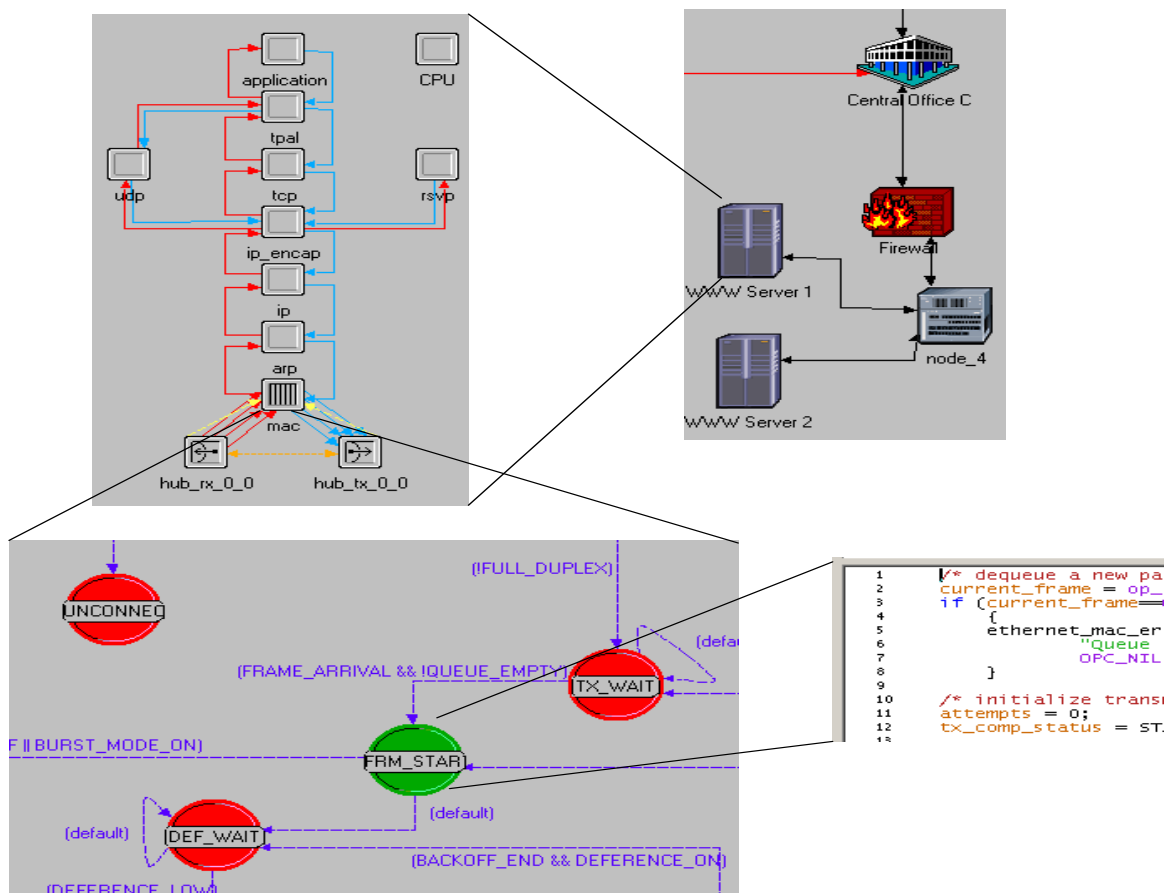
▪ توپولوژی کلی شبکه شامل گره ها ، لینک ها و... رسم می شود.

☐ Node

▪ رفتار تک تک عناصر شبکه طراحی و ترسیم می گردد

☐ Process

▪ عملکرد و رفتار هر ماژول را می توان تعریف کرد



شکل الف-۵ ساختار سلسله مراتبی در OPNET

هریک از این سه ابزار طراحی یک ویرایشگر یا Editor نامیده می شوند و در هر کدام محیطی متفاوت برای طراحی یک بخشی از مسئله آماده شده است.

## الف-۶-۱ ویرایشگر شبکه ( Network editor or Project editor )

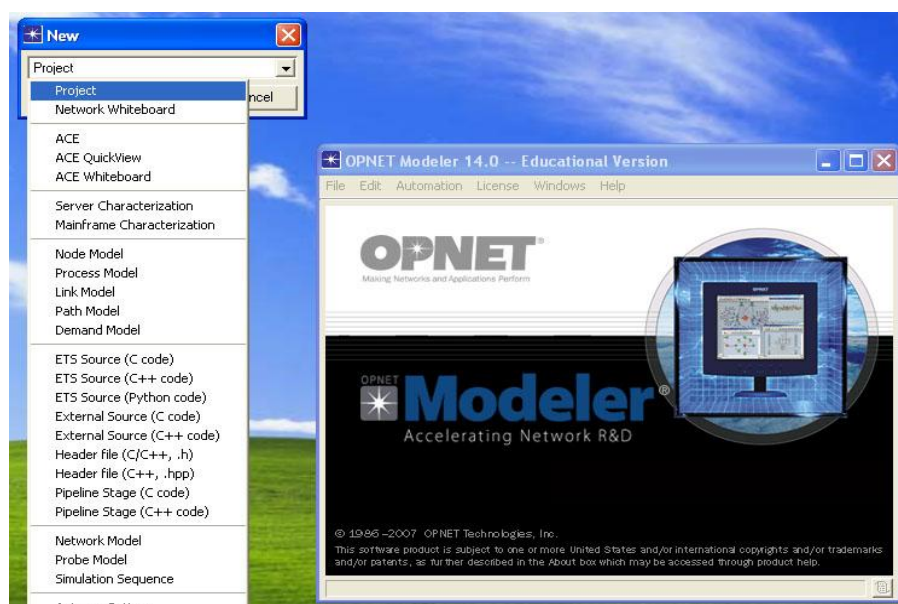
اولین مرحله شبیه سازی بوده و در آن توپولوژی کلی شبکه با استفاده از مدل هایی از جدیدترین ادوات و تجهیزات مخابراتی و شبکه که در کتابخانه این نرم افزار موجود است ، طراحی و مدل می شود. ساختار شبکه در این محیط شامل گره ها و لینک هایی است که این گره ها را به هم متصل می نماید که برای رسم این توپولوژی از پنجره Object Palette به روش کشیدن و رها کردن استفاده می گردد. همچنین برای رسم شبکه های با ابعاد وسیع در این محیط می توان موقعیت جغرافیایی شبکه را نیز به دلخواه تعیین نمود.

برای وارد شدن به محیط ویرایشگر شبکه پس از اجرای نرم افزار و باز شدن پنجره اصلی از منوی File یکی از گزینه های New یا Open را انتخاب می نمایید که با انتخاب Open می توان از مدل های موجود در کتابخانه نرم افزار استفاده کرد و با انتخاب New یک سناریوی جدید که مدنظر است را ایجاد نمود.

با انتخاب New پنجره ای باز می گردد که در آنجا باید سطح شبیه سازی را مشخص کنید که ما چون می خواهیم در سطح Project کار کنیم گزینه Project را انتخاب می نمایم.

بعد از این مرحله پنجره دیگری باز شده که در آن می توانید موقعیت جغرافیایی شبکه خود را مشخص نمایید بعد از تعیین موقعیت جغرافیایی پنجره ای باز خواهد شد که در آن باید تکنولوژی ادوات مورد استفاده برای شبیه سازی را انتخاب کنید.

آخرین پنجره ای که باز می گردد حاوی تمامی اطلاعاتی است که در مراحل قبلی انتخاب کردید و بصورت خلاصه برای تایید نهایی قرار داده شده است که بعد از تایید آن وارد محیط ویرایشگر شبکه

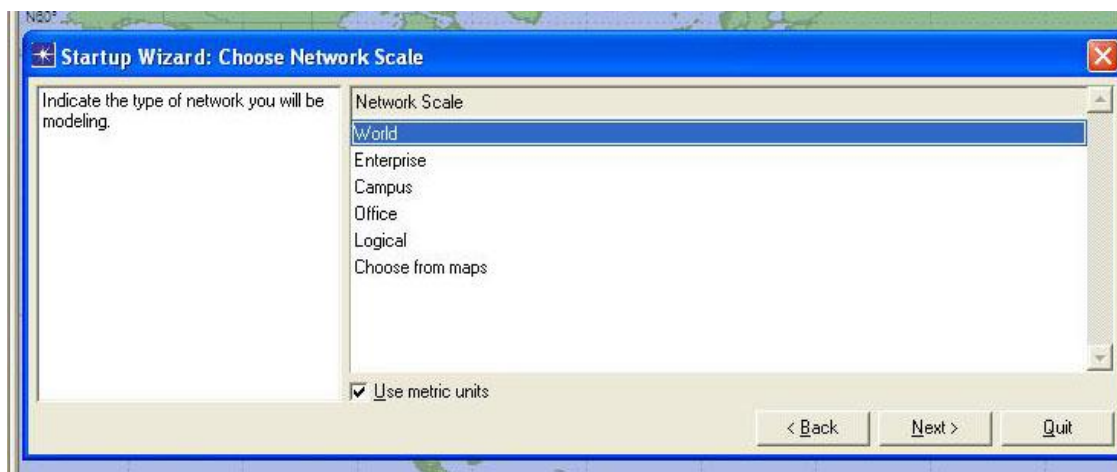


شکل الف-۶ انتخاب و وارد شدن به محیط ویرایشگر شبکه

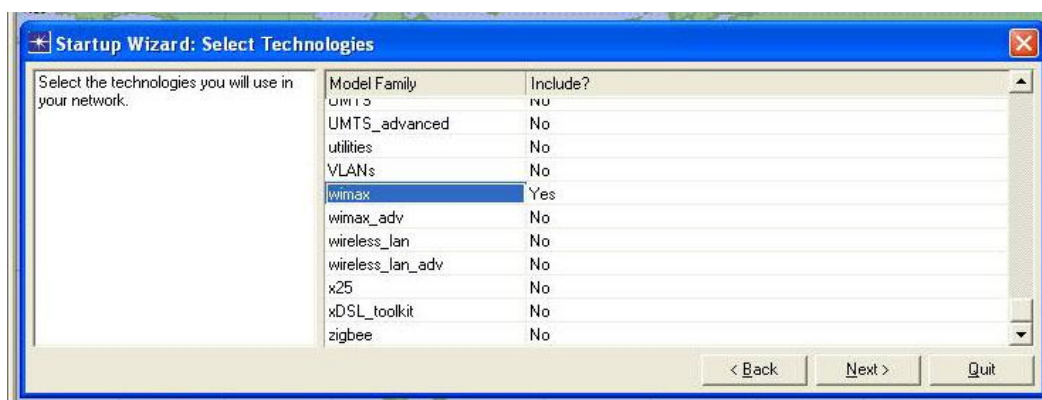


شکل الف-۷ انتخاب ساختار شبکه بر مبنای یک ساختار قبلی

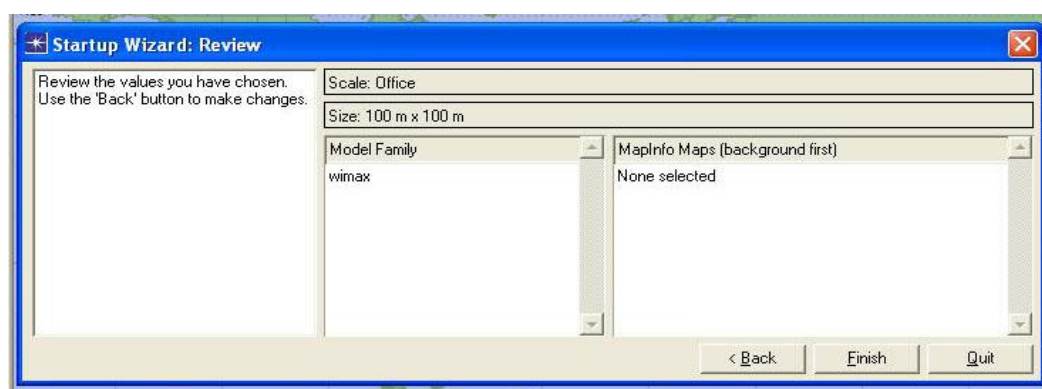




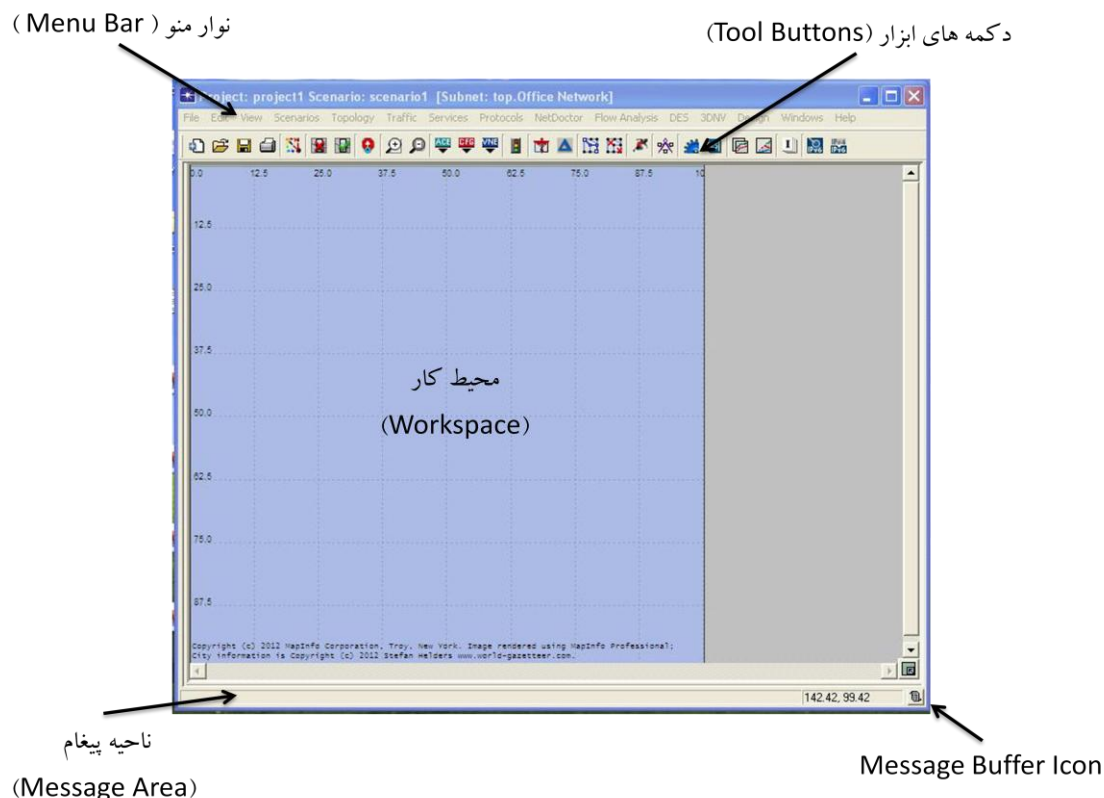
شکل الف-۸ انتخاب مشخصات جغرافیایی شبکه



شکل الف-۹ تکنولوژی ادوات مورد استفاده



شکل الف-۱۰ نمایش تمامی اطلاعات انتخاب شده در مراحل قبل برای تایید نهایی



شکل الف-۱ محیط ویرایشگر شبکه

### الف-۱-۶ پنجره Object palette

در این پنجره کلیه تجهیزات مورد استفاده در طراحی سخت افزاری شبکه شامل روتر، سوئیچ، سرور و همچنین لینک های مختلف و سایر تجهیزات شبکه ای و مخابراتی وجود دارد، ادوات موجود در Object Palette را می توان به ۴ دسته تقسیم نمود:

#### Devices ☐

- ادوات سخت افزاری نظیر روترها، سوئیچ ها و ... را شامل می شود

#### Links ☐

- لینک ها جهت اتصال گره ها به یکدیگر در تکمیل ساختار شبکه به کار می روند.

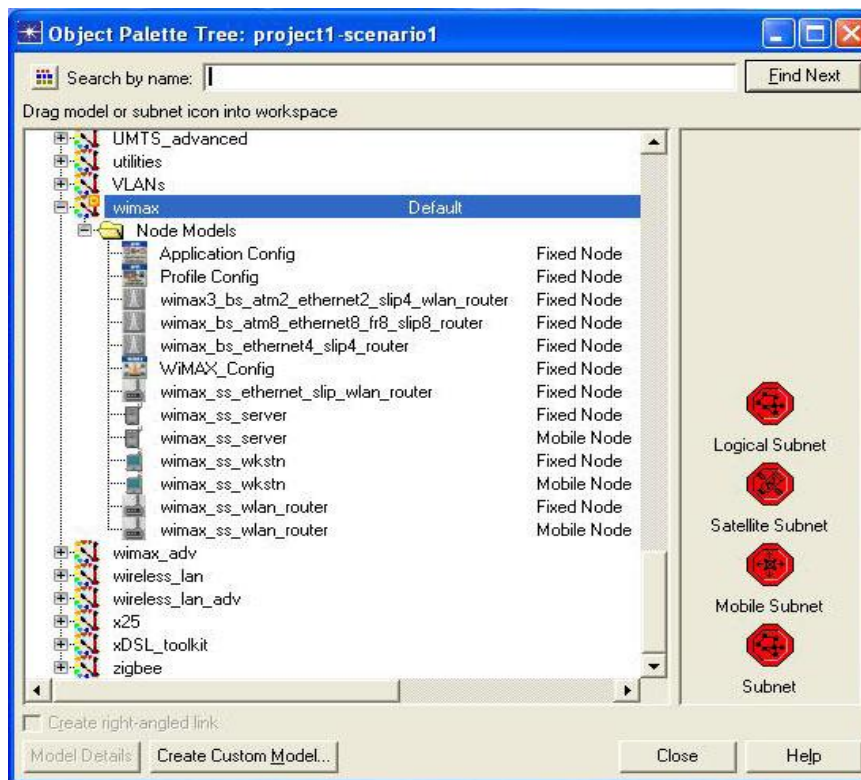
#### LANs and clouds ☐

- داشتن یک LAN ساده بصورت خلاصه در یک گره و همچنین استفاده از ابرها برای داشتن بخشی از یک شبکه WAN در یک گره که هر دو اینها جهت ساده سازی مورد استفاده قرار می گیرند.

#### Utility objects ☐

- اشیاء سودمند وظایفی که در دنیای واقعی برای آنها واحد سخت افزاری وجود ندارد را انجام می دهند بر

فرض مثال وظیفه پیکربندی منابع شبکه



شکل الف-۱۲ پنجره Object Palette

پنجره Object palette که در ورژن ۱۴ این نرم افزار ادوات بسیار زیادی قرار داده شده که بسته به تکنولوژی مورد استفاده می توانید ادوات مربوطه را نیز به راحتی مورد استفاده قرار دهید

### الف-۶-۱-۲ رسم ساختار شبکه در محیط ویرایشگر شبکه :

سه روش برای رسم توپولوژی شبکه وجود دارد :

- ☐ در روش اول می توان هر گره را لینک را بطور جداگانه از پنجره Object palette برای طراحی شبکه به محیط ویرایشگر وارد کرد.
- ☐ در روش دوم می توان از گزینه Rapid Configuration در منوی Topology استفاده کرد از این گزینه زمانی که شبکه دارای ساختاری منظم و با تعداد گره های زیاد است استفاده می گردد.
- ☐ سومین روش برای رسم ساختار شبکه در محیط ویرایشگر ، وارد کردن توپولوژی شبکه با استفاده از یک فایل خارجی است در OPNET این قابلیت وجود دارد که بتوان اطلاعات را از یک فایل خارجی به ساختار شبکه وارد کرد برای این منظور بیشتر از فایل های XML استفاده می شود.

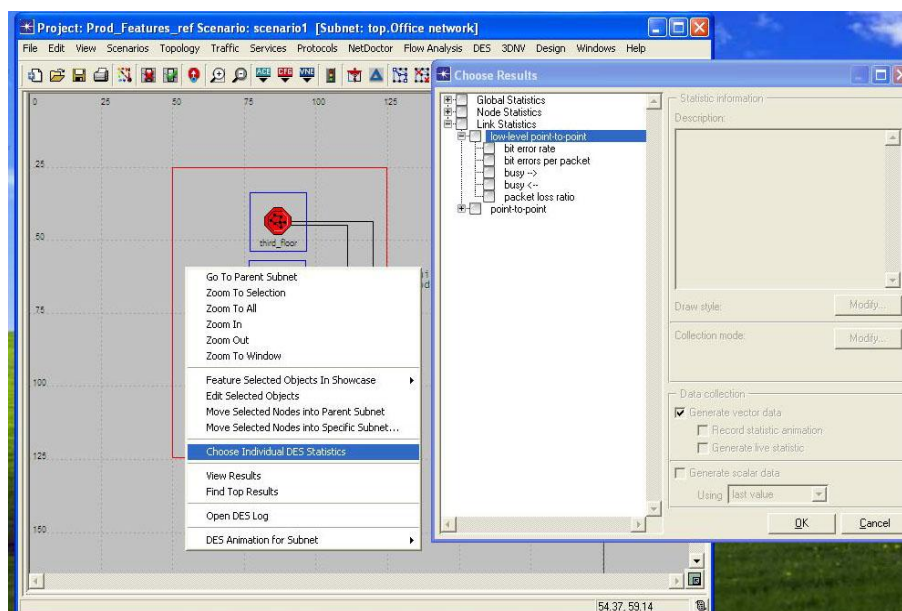
### الف-۶-۱-۳ مشخص کردن پارامترهای مورد نظر برای اجرای شبیه سازی

بعد از رسم ساختار شبکه در محیط ویرایشگر نوبت به اجرای شبیه سازی می رسد. برای این منظور ابتدا باید پارامتر یا پارامترهایی که می خواهیم تغییرات آنها را در شبکه بررسی کنیم را تعیین نماییم.

در OPNET این پارامترها را که اصطلاحاً Statistics می نامند به دو دسته تقسیم می کنند:

- ❑ پارامتری که در مورد همه ادوات شبکه صدق می کند که به آنها پارامتر عمومی (Global) گویند.
- ❑ پارامتری که مربوط به یک وسیله خاص می باشد و فقط اطلاعات از آن جمع آوری شده و نتایج گزارش شود (Object Statistics).

برای تعیین و تنظیم این پارامترها می توان از گزینه Choose individual DES statistics در منوی Simulation استفاده کرد.

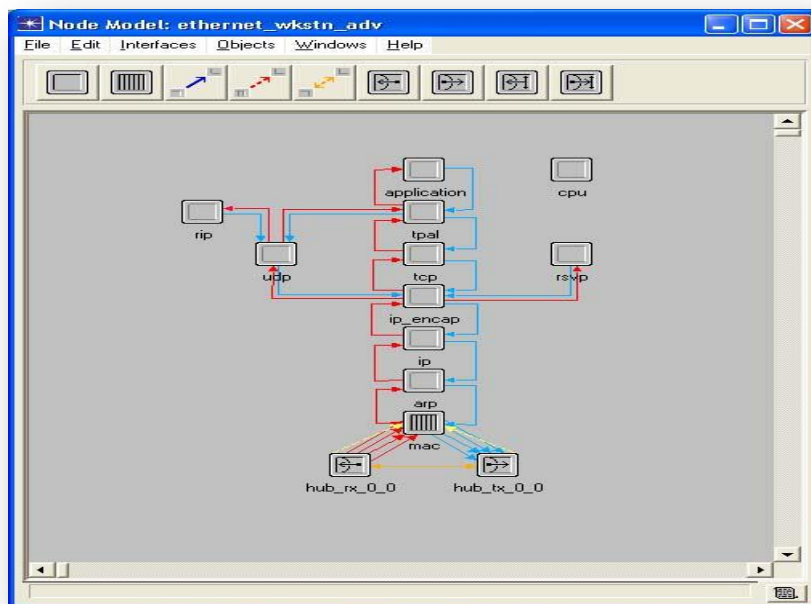


شکل الف-۱۳ تعیین پارامترهای مورد نیاز برای اجرای شبیه سازی پارامترهای خصوصی و عمومی

بعد از تعیین پارامترهای مربوطه نرم افزار آماده اجرا می باشد که برای اجرا می توان از منوی Simulation گزینه Run Simulation را انتخاب کرد یا از طریق دکمه Configure/run simulation این کار را انجام داد. بعد از این کار پنجره ای باز می شود که در آن باید تنظیمات جانبی شبیه سازی نظیر مدت زمان شبیه سازی رفتار شبکه را انجام داد. با انتخاب گزینه Run در پایین پنجره، عملیات شبیه سازی آغاز می شود.

## الف-۶-۲ ویرایشگر Node

در این ویرایشگر ساختار لایه ای تک تک عناصر شبکه و نحوه ارتباط لایه ها با یکدیگر تعیین می شود. لذا در این سطح با جریان داخلی بسته ها درون یک عنصر شبکه سرو کار داریم.



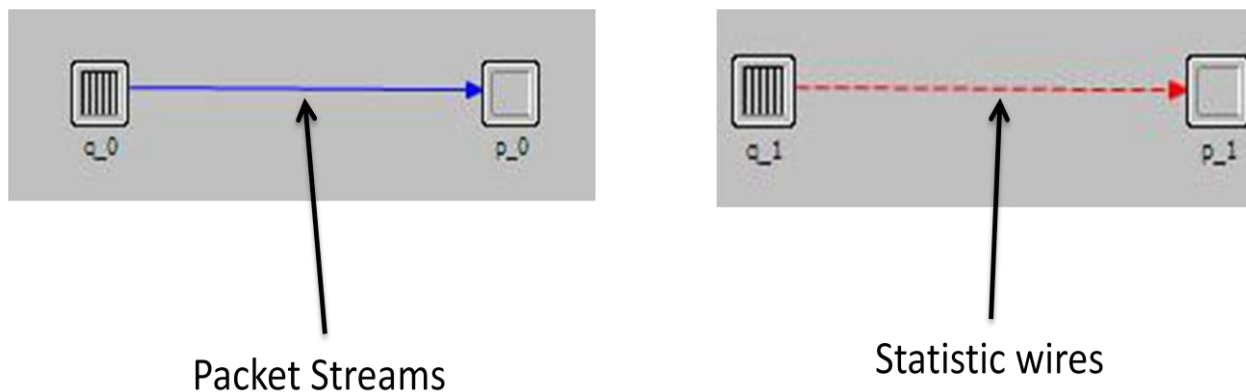
#### شکل الف-۱۴ محیط ویرایشگر Node

به طور کلی هر عنصر شبکه که دارای تمامی یا برخی از قابلیت های زیر باشد را به یک گره تعریف می کنیم: ایجاد بسته های اطلاعاتی، ذخیره آنها، ارسال و دریافت آنها و در نهایت مسیریابی داخلی و انجام پردازش های لازم نظیر آنالیز محتویات بسته ها، مالتی پلکسینگ، کشف و تحلیل خطاهای احتمالی بسته و ....

لذا هر گره شامل ادوات سخت افزاری لازم و همچنین نرم افزارهای مورد نیاز برای انجام چنین پردازش هایی است. در این ویرایشگر برای مدل کردن لایه های یک عنصر از بلوک هایی به نام ماژول استفاده می کنیم.

یک مدل در سطح Node از چندین ماژول تشکیل شده که برای عناصر پیچیده شبکه، تا چند صد ماژول هم ممکن است داشته باشیم.

ماژول ها در این ویرایشگر به وسیله Packet Streams و یا Statistic wires به یکدیگر متصل می شوند. Packet Streams اتصالاتی هستند که بسته های اطلاعاتی را از ماژول مبدا به ماژول مقصد منتقل می کنند. Statistic wires همانند قبلی اطلاعات را از یک ماژول به ماژول دیگر منتقل می کنند اما برخلاف قبلی که بسته های اطلاعاتی را منتقل می کنند، Statistic wires بسته های کنترلی که باید بین ماژول ها جهت انجام عملیات سیگنالینگ مبادله شوند را منتقل می کنند.



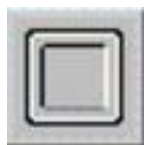
شکل الف-۱۵ انواع اتصال ماژول ها

**الف-۶-۲-۱ انواع ماژول ها در ویرایشگر Node**

به طور کلی در این ویرایشگر ۵ ماژول مختلف می توان تعریف کرد :

**ماژول پردازشگر ( Procedure Module ) :**

ماژول پردازشگر را می توان بلوک های اولیه و پایه ای برای ایجاد هر مدل در این ویرایشگر دانست. این دسته از ماژول ها برای انجام پردازش های کلی بر روی بسته های اطلاعاتی به کار می روند.



شکل الف-۱۶ ماژول پردازشگر

**ماژول صف ( Queue Module ) :**

هر ماژول صف از تعدادی زیر صف ( SubQueue ) تشکیل شده است که تعداد آنها را می توان به دلخواه تعیین کرد. هر زیر صف را می توان به طور جداگانه پیکربندی کرد.



شکل الف-۱۷ ماژول صف

**ماژول های فرستنده :**

این ماژول ها رابط بین Packet Streams درون یک گره و لینک فیزیکی خارج آن گره دانست.





فرستنده Bus



فرستنده نقطه به نقطه

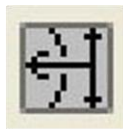


فرستنده رادیویی

شکل الف-۱۸ انواع ماژول های فرستنده

### ماژول های گیرنده :

این ماژول ها رابط بین لینک های فیزیکی و Packet Streams درون یک گره می باشند.



گیرنده Bus



گیرنده نقطه به نقطه



گیرنده رادیویی

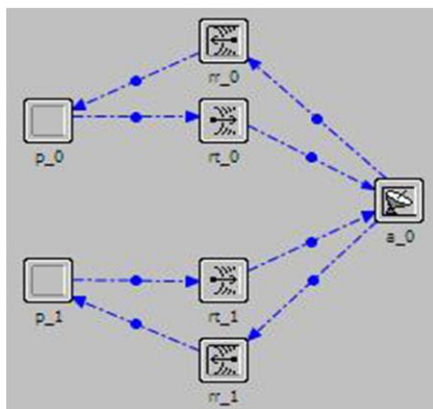
شکل الف-۱۹ انواع ماژول های گیرنده

### ماژول آنتن :

این ماژول که تنها در نسخه OPNET Modeler /Radio موجود است ، برای تعیین ویژگی های آنتن به کار رفته در ماژول فرستنده و یا گیرنده به کار می رود. با این کار می توان به طور همزمان ویژگی های یکسانی برای آنتن های فرستنده و گیرنده موجود در یک گره تعریف کرد.



ماژول آنتن



نحوه تعاملات آنتن های گیرنده و فرستنده

شکل الف-۲۰ ماژول آنتن و نحوه تعاملات آنتن ها

## الف-۶-۲-۲ منوهای مختلف در ویرایشگر Node

بعضی از منوهای موجود نیاز به توضیح خاصی ندارد نظیر File، Edit، Help برای همین در اینجا منوهای مهم تر را عنوان خواهیم کرد:

### منوی Interfaces:

این منو شامل گزینه هایی است که با استفاده از آنها می توان رابط های بین یک گره با گره های دیگر را تعریف کرد.

جدول الف-۱ گزینه های موجود در منوی interfaces

توضیح	بخش های منو
به شما اجازه ویرایش ویژگی های Node های مدل را می دهد.	Model Attributes
اجازه کنترل جنبه های مختلف ارتقاء ویژگی در سطح شبکه را می دهد	Node Interfaces
ترویج آمار ماژول انتخاب شده به سطح گره	Node Statistics
اجازه تنظیم اطلاعات گره ای که Opnet استفاده می کند را برای تطبیق مدل های گره با گره های توپولوژی وارد شده را می دهد	Self Description

### منوی Objects:

با استفاده از این منو کاربر می تواند اقدام به انتخاب ماژول های مختلف برای ایجاد یک مدل جدید کند.

این منو دارای بخش های زیر می باشد:

Create Processor، Create Queue، Create Packet Generator، Create Clocked Packet Generator، Create Packet Stream، Create Statistic Wire

### منوی Windows:

با استفاده از این منو می توان به پنجره های مربوط به سایر ویرایشگرها دست یافت و یا همزمان چندین پنجره را در صفحه به صورت آبخاری مشاهده کرد.



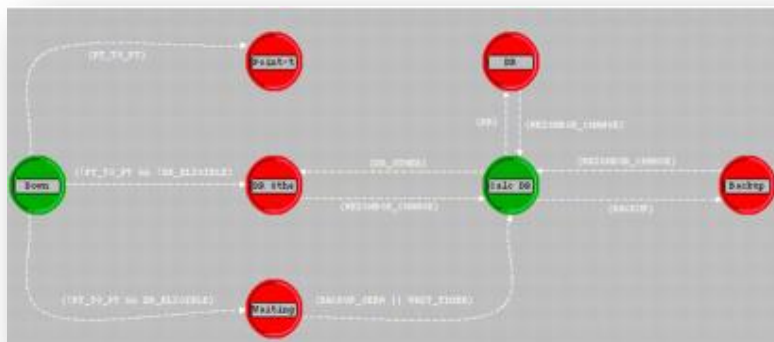
## جدول الف-۲ گزینه های موجود در منوی windows

توضیح	بخش های منو
ویرایشگر قبلی را فعال می سازد	Previous Editor
حرکت در میان ویرایشگرهای باز	Circulate Editor
ویرایشگر فعال را مخفی می کند ولی ذخیره یا عمل بستن را انجام نمی دهد	Hide This Editor
عمل بالا را برای سایر ویرایشگرها انجام می دهد	Hide Other Editors
همه ویرایشگرهای مخفی شده در قبل را نمایش می دهد	Show All Editor
پنجره سیستم را فعال می سازد	System Window
تمامی ویرایشگرهای باز را بصورت آبخاری لیست می کند	Project Editors

## الف-۶-۳ ویرایشگر Process :

در این ویرایشگر عملکرد هر ماژول تعریف می شود. شبیه سازی مدل ها در این ویرایشگر بر مبنای دیاگرام های STD صورت می گیرد. در نتیجه عملکرد هر ماژول به صورت شماتیک و کاملاً قابل درک نشان داده می شود. یک دیاگرام STD از تعدادی حالت تشکیل شده است که هر حالت با یک دایره مشخص می شود و با رخداد شرایطی خاص، گذار از حالتی به حالت دیگر صورت می گیرد.

عملکرد هر حالت توسط زبان برنامه نویسی Porto-C بیان می شود. این زبان برنامه نویسی بر مبنای زبان C بوده و با افزودن یکسری توابع خاص به آن که به آنها Kernel Procedures گفته می شود و برای شبیه سازی الگوریتم ها و پروتکل ها طراحی شده است.



شکل الف-۲۱ دیاگرام STD

### الف-۶-۳-۱ حالات موجود در دیاگرام STD

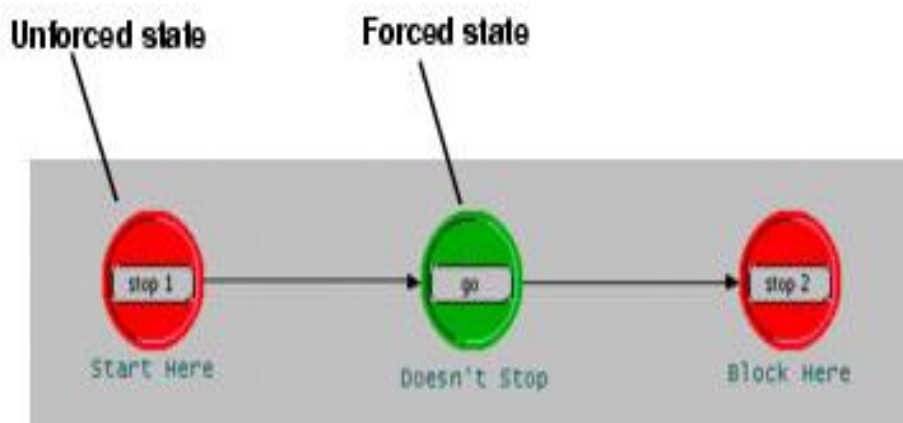
حالات موجود در دیاگرام STD به دو دسته تقسیم بندی می شوند :

#### □ حالت های اجباری یا Forced

- این حالت ها در دیاگرام موجود بصورت دایره های قرمز رنگ می باشد و حالتی است که با ورود به آن ، پس از اجرای وظایف تعریف شده مربوط به آن ، بطور خود کار به حالت دیگری می رویم.

#### □ حالت های غیر اجباری یا Unforced

- این حالت ها در دیاگرام موجود بصورت دایره های سبز رنگ می باشد و حالتی است که بعد از ورود به آنها و خاتمه انجام وظایف مربوط به آنها ، در همان حالت متوقف می شویم تا اینکه شرایط خاصی رخ دهد.



شکل الف-۲۲ حالات های موجود در دیاگرام STD

### الف-۶-۳-۲ بررسی منوهای موجود در ویرایشگر Process

منوهای **File** ، **Edit** ، **Help** که نیاز به توضیح خاصی ندارند.

**منوی Interfaces** : این منو شامل گزینه هایی است که با استفاده از آنها کاربر می تواند رابط های بین یک مدل با مدل های دیگر را تعریف کند.

**منوی FSM** : برای ایجاد یک دیاگرام STD استفاده می شود و برخی از گزینه های آن عبارتند از : ایجاد حالت ، ایجاد خط گذار و تنظیم حالت اولیه دیاگرام.

**منوی Code Blocks** : با استفاده از این منو می توان به متغیرها ، توابع مورد استفاده و بطور کلی تمامی موارد مربوط به برنامه C نوشته شده برای مدل مربوطه دسترسی داشت.

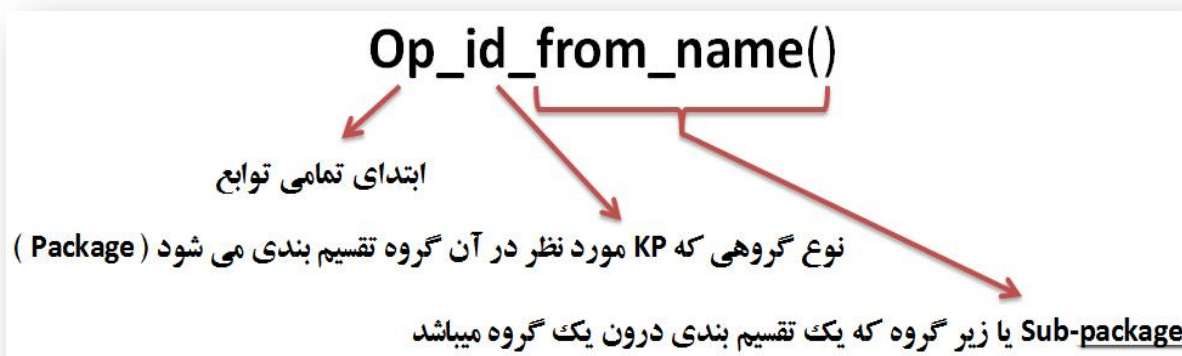
**منوی Compile :** شامل گزینه هایی برای کامپایل کردن برنامه های نوشته شده ، پیدا کردن خطاها ، اصلاح و کامپایل دوباره برنامه می باشد.

**منوی Windows :** با استفاده از این منو می توان به پنجره های مربوط به سایر ویرایشگرها دست یافت و یا همزمان چندین پنجره را بصورت آبشاری مشاهده کرد.

### الف-۶-۳-۳ تعریف شده در Porto-C

زبان Porto-C بر مبنای زبان C و با افزودن یکسری توابع خاص با عنوان KP طراحی شده است و کاربرد آن در شبیه سازی پروتکل ها و الگوریتم ها می باشد و برای همین برای آن دیاگرامهای STD در نظر گرفته شده است .

نام این توابع KP دارای چند قسمت است :



شکل الف-۲۳ نحوه نامگذاری توابع KP

برخی از مهمترین گروههای KP

**Animation Package** □

با حروف اختصاری Anim که برای انجام عملیات خلق تصاویر انیمیشن در حین اجرای شبیه سازی به کار می روند.

**Distribution Package** □

با حروف اختصاری Dist برای تولید و ایجاد مقادیر تصادفی ( آماری ) بر مبنای توزیع احتمال مشخص مثل توزیع یکنواخت یا توزیع نمایی سروکار دارند و بیشتر برای تولید پارامترهای تصادفی استفاده می شوند.

**Event Package** □

با حروف اختصاری ev می باشد که این توابع با رویدادهای اتفاق افتاده در طول یک شبیه سازی سروکار دارند به عنوان مثال با استفاده از آنها می توان به حذف و لغو رویدادهایی که وجود آنها بیش از این مورد نیاز نیست اقدام کرد مثلاً در TCP هنگامی که منتظر دریافت پیام Ack از سوی گیرنده هستیم ، رویداد time out را هم مد نظر قرار می دهیم تا اگر بعد از مدت زمان مشخص این پیام رسید time out رخ دهد اما اگر پیام Ack قبل از موعد مقرر برسد فرآیند time out باید لغو شود که این کار توسط op\_ev\_cancel() صورت می گیرد.

### Interrupt Package □

برای تنظیم و زمان بندی وقوع وقفه های ورودی و خروجی به کار می رود و با اختصار intrpt نوشته می شود.

### Identification Package □

برای دریافت شماره id هر شیء که در شبیه سازی ایجاد شده است به کار می رود. مثلاً  
op\_id\_from\_name ، نام متغیر را به عنوان آرگومان ورودی خود دریافت نموده و وظیفه تبدیل نام شیء مربوطه به شماره آن را برعهده دارد.

### Queue Package □

مربوط به عملیات صف بندی می شود. مثلاً op\_q\_empty برای پی بردن به این نکته که صف خالی است یا خیر به کار می رود و یا op\_q\_flush برای خالی کردن یک صف زمانی که بسته های موجود در صف دچار خطا شده اند به کار می رود

### Radio Package □

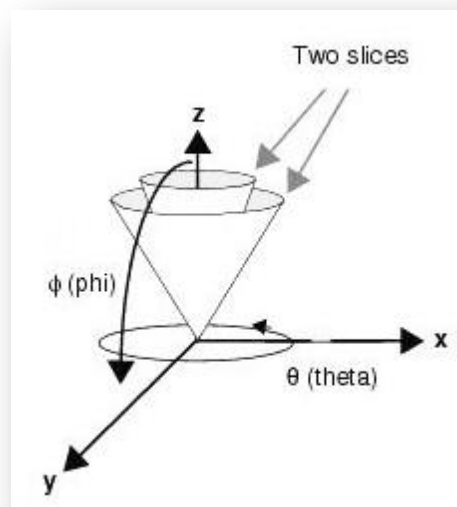
با مازول های فرستنده و گیرنده در ارتباط هستند و با استفاده از آنها می توان به صورت دینامیک کانال های مورد استفاده توسط یک فرستنده را تغییر داد مثلاً اضافه یا حذف یک کانال را با استفاده از این توابع انجام داد.

### Packet Package □

با نام اختصاری pk می باشند و برای انجام عملیات بر روی بسته ها مورد استفاده قرار می گیرند

## الف-۷ ویرایشگر انتشار آنتن (Antenna Pattern Editor)

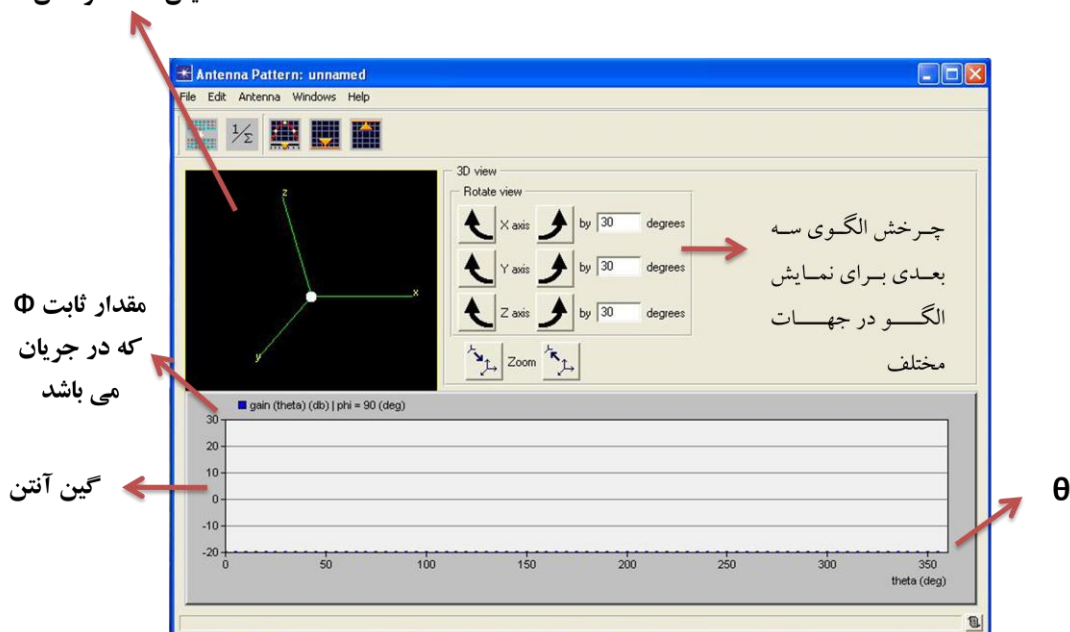
- ویرایشگر الگوی آنتن از زوایای  $\Phi$  و  $\theta$  برای ایجاد و نمایش سه بعدی الگوی آنتن استفاده می نماید.
- مقدار ثابت  $\Phi$  بطور تقریبی سطوح مخروطی شکل دو بعدی را نمایش می دهد که داخل مختصات دکارتی نگاشته شده و توسط توابع عددی دو بعدی رسم شده اند که به آنها Slice یا Plane گفته می شود.
- $\theta$  محور طول و گین محور عرض در هر Slice می باشد.
- تابع سه بعدی الگوی آنتن با جمع آوری Slice های دوبعدی نمایش داده می شود.



شکل الف-۲۴ نمایش پارامترهای ویرایشگر انتشار آنتن

محیط ویرایشگر انتشار آنتن

نمایش 3D الگو آنتن



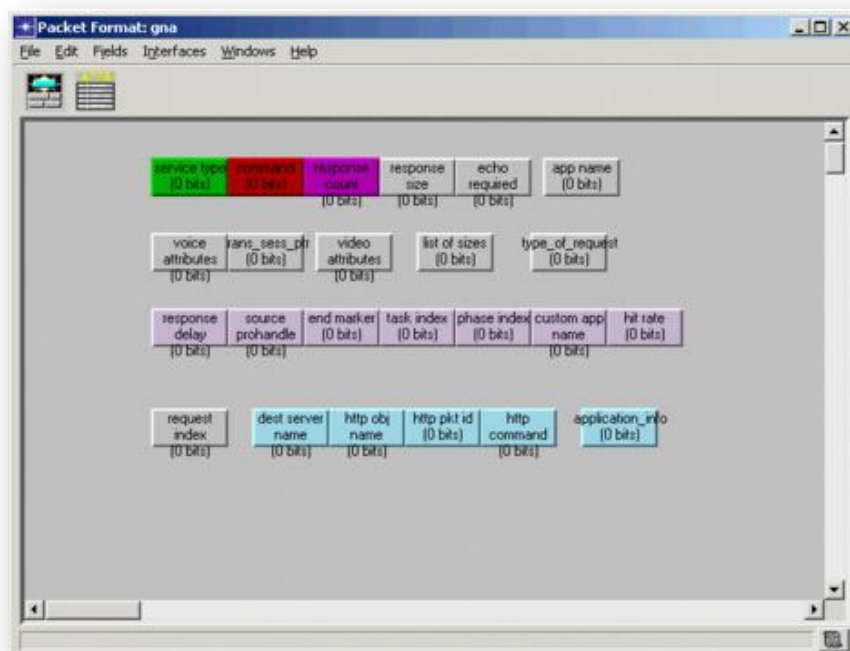
شکل الف-۲۵ محیط ویرایشگر آنتن

## الف-۸ ویرایشگر فرمت پکت (Packet Format Editor)

این ویرایشگر امکان ایجاد و ویرایش فرمت پکت ها مطابق با آنچه طراح مد نظر دارد را فراهم می کند.

پکت ها از فیلدهایی تشکیل شده که در این ویرایشگر می توان مشخصات فیلدها را مطابق با آنچه مد نظر است مشخص کرد.

انواع فیلدها در این ویرایشگر عبارتند از: integer, double, structure, information, Packet که بر فرض مثال فیلد structure اجازه گنجاندن و قرار دادن داده های مختلط را در فیلد می دهد یا فیلدهای information داده ها را بدون در نظر گرفتن محتوای آنها به صورت عمده ای مدل می کنند یا فیلد های packet پکت ها را با تلفیق داده های دیگر، توسط پروتکل های لایه بندی مدل می کند. (داده ها را با هم کپسوله می کنند).



شکل الف-۲۶ محیط ویرایشگر Packet Format

## الف-۸-۱ عملیات ویرایشگر فرمت پکت

عملیاتی که در این ویرایشگر انجام می شود به طور کلی عبارتند از:

- ایجاد فیلد جدید

ایجاد نمایش گرافیکی از فیلدهای جدید و قرار دادن آنها در فضای کاری یا workspace

- ویرایش صفات فیلد

نمایش یا تغییر ویژگی های یک فیلد، تغییرات ایجاد شده در یک فیلد می تواند به طور اختیاری به کل مجموعه فیلدها اعمال شود.

- ویرایش ویژگی های پکت

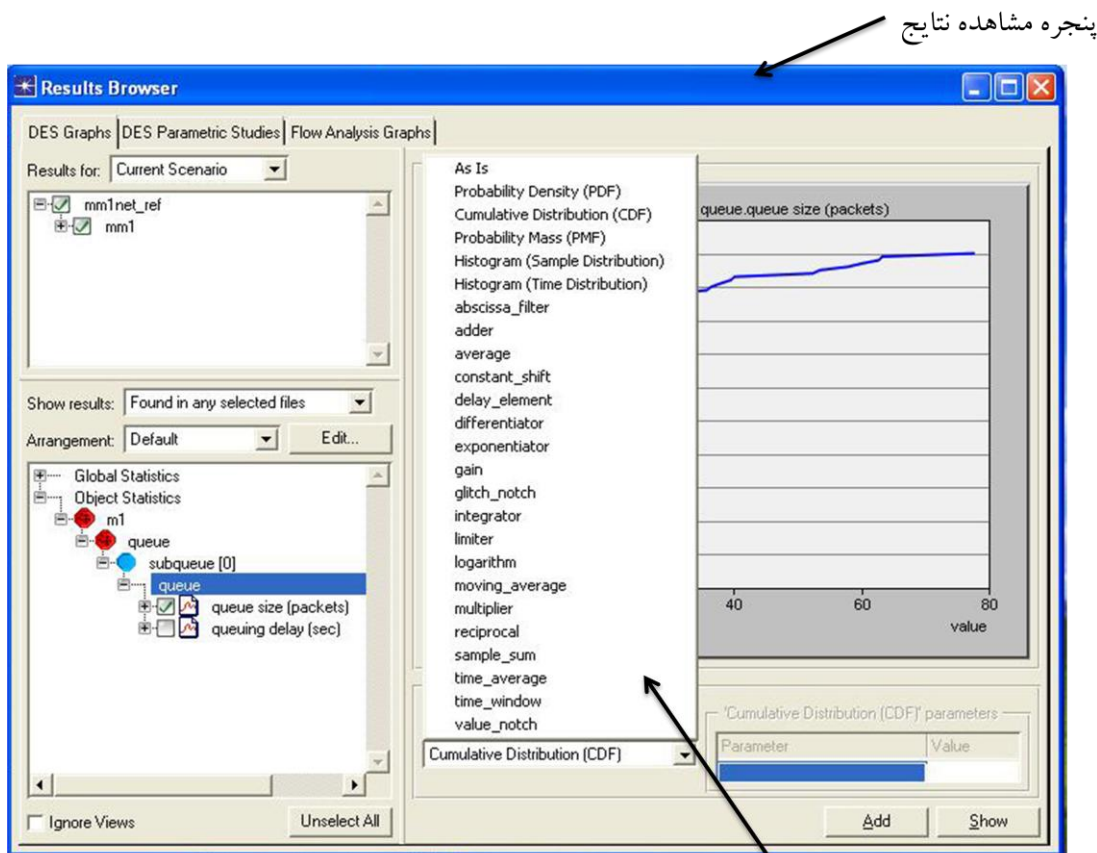
نمایش یا تغییر ویژگی های مربوط به کل بسته است .

## الف-۹ مشاهده و تحلیل نتایج شبیه سازی

بعد از اینکه مدل مربوطه را توسط دکمه Configure/run simulation اجرا کردیم حال باید نتایج آن را مشاهده نماییم که برای این کار از گزینه View results موجود در منوی Result استفاده می کنیم یا روی هر نود کلیک راست کرده و مشاهده نتایج را انتخاب می نماییم.

برای مشاهده کل نتایج باید روی ناحیه کاری جایی که هیچ نودی قرار ندارد راست کلیک کرده و مشاهده نتایج را انتخاب نماییم که با انتخاب آن پنجره نتایج باز می شود که در آن می توان آمار عمومی یا آمار مربوط به هر نود را انتخاب نمود.

از دیگر قابلیت های این نرم افزار در بررسی نتایج ، امکان مقایسه نتایج سناریوهای مختلف با یکدیگر است که برای این کار از گزینه Compare Result موجود در منوی Result استفاده می گردد.



حالات مختلف برای مشاهده نتایج آماری

شکل الف-۲۷ پنجره مشاهده نتایج

## منابع :

- [۱] تنبام ، اندرواس . شبکه های کامپیوتری ، ترجمه پدرام، حسین ؛ ملکیان ، احسان ؛ زارع پور ، علی ، ویراست ۴ . تهران: انتشارات نص ، بهار ۱۳۸۷ .
- [۲] ملکیان ، احسان . اصول مهندسی اینترنت ، چاپ اول . تهران : انتشارات نص ، زمستان ۱۳۸۰ .
- [۳] رحمانی منش ، محمد ؛ عارف نسب ، محمد علی ؛ صابری ، محسن . مروری بر شبیه سازهای شبکه ، چاپ اول . تهران : شرکت ناقوس اندیشه ، ۱۳۸۷ .
- [۴] فرزین ، مهنا . شبیه سازی شبکه به کمک نرم افزار OPNET ، چاپ اول . تهران: نشر پژوهشی نوآوران شریف ، ۸۹-۹۰ .
- [۵] [لاری.ال.پیترسون ، بروس.اس.دیوی . آموزش جامع شبیه سازی شبکه با استفاده از نرم افزار OPNET ، ترجمه پورمینا ، محمدعلی ؛ فولادیان ، مجید ؛ نوری ، سارا ، چاپ اول . انتشارات قدیس ، ۱۳۹۱ .
- [۶] مهدی رجب زاده ، زینب سام دلیری . " ارزیابی و تحلیل کارائی پروتکل های مسیریابی در شبکه های اقتضائی " . همایش منطقه ای برق و کامپیوتر، دانشگاه آزاد اسلامی واحد نکاء .
- [۷] محمدحسین یغمائی ، نوشین موسوی راد . " طراحی و پیاده سازی یک پروتکل مسیریابی On\_demand برای شبکه های MANET " . چهاردهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران ، ۲۰ و ۲۱ اسفندماه ۱۳۸۷ ، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)، ۱۳۸۷ .
- [۸] محمد رضائی، محمدحسین یغمائی،صادق زینلی . "مسیریابی مبتنی بر کیفیت سرویس در شبکه های موردی" . چهاردهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران ، ۲۰ و ۲۱ اسفندماه ۱۳۸۷ ، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)، ۱۳۸۷ .
- [۹] مسیح موسی پور . امنیت مسیریابی در شبکه های موردی .سمینار درس کارشناسی ارشد.دانشگاه صنعتی امیرکبیردانشکده مهندسی کامپیوتر و فناوری اطلاعات، ۱۳۸۴ .
- [۱۰] بهمن مددی ، علیرضا جلفایی ، علی عطاران ، سوده نیکان . " یک روش بهینه مسیریابی در شبکه های Ad hoc " .

[11] Sajjad Ali & Asad Ali , " Performance Analysis of AODV, DSR and OLSR in MANET " , Department of Electrical Engineering with emphasis on Telecommunication Blekinge Institute of Technology, Sweden 2009 .

[12] Jahangir khan<sup>†</sup>, Dr.syed Irfan Hyder<sup>††</sup>, Dr.Syed Malek Fakar Duani syed Mustafa<sup>†</sup>, "Modeling and Simulation Of Dynamic Intermediate Nodes And Performance Analysis in MANETS Reactive Routing protocols " , School of Information & communication Technology<sup>†</sup>, Asia e University, No. 4, Jalan Sultan Sulaiman, 50000 Kuala Lumpur, Malaysia.Graduate School of science & Engineering<sup>††</sup>, March 2011 .

[13]Anipakala Suresh , " Performance Analysis of Ad hoc On-demand Distance Vector



- routing (AODV) using OPNETSimulator ", Communication Networks University of Bremen, 11 April 2005 .
- [14] Mehran Abolhasan et al, "A review of routing protocols for mobile ad hoc networks " Ad Hoc Networks 2004 (1-22) .
- [15] Laura M. Feeney, "A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks", Technical Report .
- [16] Avinash Kasyap et al, "Survey on Unicast Routing in Mobile Ad Hoc Networks", 2001 .
- [17] E. Boyer and C. Toh, "A review of current routing protocols for Ah Hoc Mobile Wireless Networks", IEEE personal Communications, April 1999 .
- [18] [PPT] Reza.Mohammadi , OLSR (Optimized Link State Routing) .
- [19] [PPT] Spanakis Manolis ,Mobile Ad-hoc Networks Routing Protocols , CS539 Computer Science Department 16/03/2005 .
- [20] opnet tutorial-Creating a Wireless Network .
- [21] OPNET Modeler 14.5 Help .
- [22] <http://ad-hoc.blogfa.com/visited> on 12/11/2011 .
- [23] <http://computer.parsx.com/forum-6.html> visited on 12/11/2011.
- [24] <http://baladorprojects.blogfa.com/> visited on 7/10/2012 .
- [25] <http://baladorprojects.blogfa.com/post-6.aspx> visited on 7/10/2012 .
- [26] <http://www.pjiran.ir/forum/forum600/thread9978.html> visited on 8/1/2012 .
- [27] <http://www.adhak.parsiblog.com/> visited on 8/1/2012 .
- [28] <http://www.ecg-pnum.com/> visited on 8/1/2012 .
- [29] <http://www.pjiran.ir/forum/forum600/thread3287.html> visited on 8/1/2012 .
- [30] <http://ee.sharif.ir/~farhat/networking/adhoc/ad-hoc%20networks%20security.htm> visited on 8/1/2012 .
- [31] [wimax.blogfa.com](http://wimax.blogfa.com) visited on 8/1/2012 .
- [32] <http://mina89.blogfa.com> visited on 9/2/2012 .
- [33] <http://wiki.uni.lu/secan-lab/Dynamic+Source+Routing.html> visited on 9/2/2012 .
- [34] [http://w3.antd.nist.gov/wctg/manet/manet\\_bibliog.html#Model](http://w3.antd.nist.gov/wctg/manet/manet_bibliog.html#Model) visited on 9/2/2012.
- [35] <http://library.sharif.ir> visited on 9/3/2012 .
- [36] <http://wdl.persiangig.com/pages/download/?dl=http://jtriplej.persiangig.com/opnet.rar> visited on 9/3/2012 .
- [37] <http://northcomputer.persianblog.ir/post/3> visited on 9/3/2012 .
- [38] [http://confbank.um.ac.ir/modules/conf\\_display/conferences/ikt07/pdf/F2\\_1.pdf](http://confbank.um.ac.ir/modules/conf_display/conferences/ikt07/pdf/F2_1.pdf) visited on 9/3/2012 .
- [39] <http://rasouli.iranweb3.com> visited on 9/3/2012 .
- [40] <http://www.aghazeh.com/computer-network-ebooks/642.html> visited on 9/3/2012.
- [41] <http://mohandesyar.com> visited on 9/4/2012 .
- [42] <http://www.iran-eng.com> visited on 12/11/2011 .
- [43] <http://www.scribd.com> visited on 12/11/2011 .
- [44] <http://www.njavan.com> visited on 12/11/2011 .
- [45] [cisco.parsfa.com/post-50102.html](http://cisco.parsfa.com/post-50102.html) visited on 9/4/2012 .
- [46] <http://www.forum.persianadmins.ir/showthread.php?t=4911> visited on 12/11/2011.

- [47] ee.sharif.ir/~farhat/security/rpsan.ppt visited on 8/1/2012 .
- [48] <http://www.faaq.mihanblog.com/post/72> visited on 9/3/2012 .
- [49] <http://www.faaq.mihanblog.com/post/71> visited on 9/3/2012 .
- [50] pakdaman-shz.persiangu.com/Ad-Hoc-2.doc visited on 12/10/2011 .
- [51] ceec2011.iauneka.ac.ir/getpaper.php?file=217 visited on 9/3/2012 .
- [52] [http://kettering.academia.edu/ShervinEhrampoosh/Teaching/20538/EHRAMPOOSH\\_FINAL\\_DRAFT\\_PROJECT\\_PARALLEL\\_PROCESSING\\_Ad\\_Hoc](http://kettering.academia.edu/ShervinEhrampoosh/Teaching/20538/EHRAMPOOSH_FINAL_DRAFT_PROJECT_PARALLEL_PROCESSING_Ad_Hoc) visited on 12/11/2011 .
- [53] <http://thesis.ecg-pnum.com> visited on 8/1/2012 .
- [54] [http://ceit.aut.ac.ir/~dehghan/Students/Baktash/seminar doc.pdf](http://ceit.aut.ac.ir/~dehghan/Students/Baktash/seminar%20doc.pdf) visited on 9/3/2012.
- [55] <http://network-install.blogfa.com/page/opnet> visited on 12/10/2011 .
- [56] RfC 3626 , Optimized Link State Routing Protocol(OLSR) .
- [57] RFC 3561 , Ad hoc On-Demand Distance Vector Routing (AODV).
- [58] RFC 4728 , The Dynamic Source Routing Protocol (DSR) .