
بسم الله الرحمن الرحيم

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز

رساله دکتری

مدل سازی و ارزیابی عملکردشبکه‌های موردی سیار درمقابل حمله ها با استفاده از شبکه‌های پتری

نگارنده: میثم یداله زاده طبری

استاد راهنما

دکتر علی اکبر پویان

استاد مشاور

دکتر امیدرضا معروضی

شهریور ۱۳۹۵

باسمه تعالی

شماره:

تاریخ:

ویرایش:

مدیریت تحصیلات تکمیلی

رساله دکتری آقای میثم یداله زاده طبری به شماره دانشجویی ۹۱۲۲۵۵۸۵ تحت عنوان مدل سازی و ارزیابی شبکه های موردی سیار در مقابل حملات با استفاده از شبکه های پتری توسط کمیته تخصصی زیر جهت اخذ مدرک دکتری مورد ارزیابی و با درجه --------- مورد ارزیابی قرار گرفت

استاد راهنما	دکتر علی اکبر پویان	
نماینده تحصیلات تکمیلی	دکتر حمید حسن پور	
استاد مشاور	دکتر امیدرضا معروضی	
استاد داور	دکتر مرتضی زاهدی	
استاد داور	دکتر هدی مشایخی	
استاد داور	دکتر عباس دیده بان	

تقدیم به پدر و مادر عزیزم

که هیچ کلامی گویای سپاسشان نیست. آنچه که به آن رسیدم بدون دعای خیرشان ممکن نبود

تقدیم به همسر عزیزم

به خاطر تمام محبت ها و فداکاری هایی که در حقم روا داشته و می دارد

و پدر و مادر عزیزشان به خاطر تمام حمایت های بی دریغ‌شان

و

پسرم ماهان

آنچه که اکنون برایش آرزو دارم تنها سلامتی است و برای آینده اش یک دنیا موفقیت و پیدا کردن راه دشوار زندگی

تشکر و قدردانی

در تهیه این رساله برخود لازم می دانم از زحمات استاد راهنمای گرانقدرم **جناب آقای دکتر پویان** تشکر نمایم. بدون شک، این تحقیق بدون راهنمایی های ایشان چه در مرحله معرفی موضوع و چه در طول انجام مراحل کار به سرانجام نمی‌رسید. آن‌چه که من از ایشان آموختم نه فقط درس علم بود، بلکه در طی این سال‌ها از ایشان درس اخلاق، بزرگواری و در یک کلام درس استادی آموختم.

خدا را شکر می‌گویم که فرصت آشنایی و شاگردی ایشان را برایم فراهم ساخت.

همچنین لازم است مراتب تشکر و قدردانی خود را از استاد عزیزم **جناب آقای دکتر معروضی** به عنوان استاد مشاور به‌خاطر تمام زحماتی که در طی مراحل انجام رساله تقبل فرمودند ابراز نمایم.

تعهدنامه

اینجانب میثم یداله زاده طبری دانشجوی دوره دکتری رشته مهندسی کامپیوتر گرایش هوش مصنوعی دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی شاهرود نویسنده پایان نامه با عنوان مدل سازی و ارزیابی شبکه های موردی سیار در مقابل حملات با استفاده از شبکه های پتری تحت راهنمایی آقای دکتر پویان متعهد می شوم.

- تحقیقات این پایان نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش های محققان دیگر به مرجع مورد استفاده استناد شده است.
- مطالب مندرج در پایان نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده استو
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می باشد و مقالات مستخرج با نام "دانشگاه صنعتی شاهرود" و یا "Shahrood University of Technology" به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آوردن نتایج اصلی پایان نامه تأثیرگذار بوده اند در مقالات مستخرج از پایان نامه رعایت می گردد.
- در کلیه مراحل انجام این پایان نامه، در مواردی که از موجود زنده (یا بافت های آن) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است.
- در کلیه مراحل این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری، ضوابط و اصول اخلاقی رعایت شده است.

تاریخ

امضای دانشجو

چکیده

شبکه‌های موردی سیار حاوی مجموعه ای از گره[1]ها هستند که می توانند آزادانه بدون داشتن هیچ‌گونه زیرساخت شبکه‌ای از پیش تعریف شده، با یکدیگر در ارتباط باشند. ارزیابی کارایی و خصوصیات این نوع شبکه‌ها از حیث امنیت و قابلیت اعتماد در مقابل حمله‌های وارده به آن ضروری می‌باشد. در ادبیات غالب موضوع، استفاده از شبیه سازهای سنتی مانند NS-2، Opnet اغلب دارای مشکلاتی مثل زمان‌بر بودن استخراج معیارهای ارزیابی، نوسان و تغییر نتایج خروجی و پیچیدگی کار با کدها و دستورات موجود در آن برای یک تحلیلگر می‌باشد. در مقابل، روش‌های رسمی و مدل‌سازی تحلیلی مانند شبکه‌های پتری دارای امکانات مناسبی جهت مدل‌سازی و ارزیابی یک سیستم پیچیده با مجموعه‌ای از فرآیندهای موازی می باشند. استفاده از این روش‌ها در تحلیل و ارزیابی یک سیستم دارای مزایایی مانند سرعت در استخراج نتایج، امکان تحلیل حالت پایدار سیستم و ارائه یک نمایش بصری از نحوه کارکرد آن است. همچنین استفاده از این تکنیک‌ها در طراحی پروتکل‌های مسیریابی سبب کاهش زمان توسعه، پیدا کردن اشکالات طراحی و ارزیابی دقیق و جامع آن می شود. به دلیل پیچیدگی‌های ریاضی اولیه طراحی، تلاش های کمی به‌منظور استفاده از این روش‌ها جهت مدل‌سازی و ارزیابی شبکه‌ها به‌ویژه شبکه‌های موردی سیار صورت گرفته است.

در این تحقیق ارزیابی عملکرد شبکه های موردی سیار در دو لایه شبکه و پیوند داده در مقابل حملات وارده به آن با استفاده از روش مدل‌سازی تحلیل انجام شده است. مدل سازی فرآیند کار با استفاده از کلاسی از شبکه پتری به نام شبکه تصادفی مبتنی بر پاداش (Stochastic Reward Net) صورت گرفته که در واقع نوع کامل‌تری از شبکه پتری تصادفی تعمیم یافته (Generlized Stochastic Petri net) می باشد. مدل ارائه شده وابسته به محاسبات ریاضی جهت تخمین مواردی

[1] node

مانند تعداد گام لازم جهت رسیدن بسته به مقصد، تعداد گره‌های موجود در یک فضای همسایگی و فرکانس خرابی و بازیابی یک مسیر انتقال داده می‌باشد، که در متن این رساله راه‌حلی برای هریک ارائه شده است. به‌منظور ارزیابی صحت مدل ارائه شده در این تحقیق، از روش ارزیابی مقایسه‌ای استفاده شده است. به همین منظور با تعریف سناریوهای پیاده‌سازی مشخص در شبیه ساز NS-2 و نگاشت آن در مدل ارائه شده، نتایج به ازای معیارهای ارزیابی کارایی مانند توان گذردهی و تأخیر ارسال گام به گام برای لایه پیوند داده نرخ تحویل بسته و تأخیر انتها به انتها برای لایه شبکه در دو محیط محاسبه شده اند. نتایج بدست آمده حاکی ار آن است که حمله دستکاری مکانیزم انتظار تعویق و دستکاری بازه انتظار DIFS بیشتر از سایر حملات لایه پیوند داده تأثیرگذار بوده. با فرض متخاصم بودن ۱۵٪ از گره‌های شبکه اعمال این حملات به میزان تقریباً ۳۵٪ از توان گذردهی لایه پیوند داده خواهند کاست و متوسط زمان تأخیر گام به گام را نیز تا سه برابر افزایش خواهند داد. معیارهای ارزیابی لایه شبکه به ازای اعمال سه سطح از حملات که در آن به ترتیب ۱۰٪ ، ۱۵٪ و ۲۰٪ از گره‌های متخاصم در شبکه وجود دارند محاسبه شده اند که حاکی از قدرت اثرگذاری بیشتر برای حمله سیاهچاله بوده است. معیارهای ارزیابی کارایی از مدل SRN ارائه شده در زمان بسیار کوتاهی در مقایسه با شبیه ساز NS-2 استخراج شده است. همچنین، نتایج حاکی از انطباق مقادیر دو محیط بوده است.

کلمات کلیدی:

شبکه‌های موردی سیار، شبکه‌های پتری، مدل‌سازی و ارزیابی کارایی، امنیت، حمله

لیست مقالات ژورنالی مستخرج از رساله

Pouyan A., Yadollahzadeh Tabari M. (2014) ”Estimating Reliability in Mobile ad-hoc Networks Based on Monte Carlo Simulation”, IJE TRANSACTIONS B: Applications, 27(5), PP 739-746, Scopus,

Pouyan A. A. and Tabari M. Y, (2015).” FPN-SAODV: using fuzzy petri nets for securing AODV routing protocol in mobile Ad hoc network, Int. J. Commun. Syst., Wiely,IF=1.16

فهرست مطالب

فصل ۱- مقدمه ۱

۱-۱- توضیحات موضوع و ضرورت انجام آن..... ۲

۱-۲- اهداف و روش ۴

۱-۳- فرضیات تحقیق ۶

۱-۴- چالش‌ها ۶

فصل ۲- ادبیات تحقیق ۹

۲-۱- شبکه‌های موردی سیار ۱۰

۲-۱-۱- مشخصات شبکه‌های موردی سیار ۱۱

۲-۱-۲- پشته پروتکلی در شبکه‌های موردی سیار ۱۴

۲-۱-۲-۱- لایه شبکه در شبکه‌های موردی سیار ۱۷

۲-۱-۲-۲- پروتکل‌های پیش کنشی ۱۸

۲-۱-۲-۳- پروتکل‌های واکنشی ۱۸

۲-۱-۲-۴- پروتکل‌های ترکیبی ۲۴

۲-۱-۲-۵- حملات لایه شبکه ۲۵

۲-۱-۳- لایه پیوند داده ۲۸

۲-۱-۳-۱- پروتکل IEEE 802.11 DCF ۳۱

۲-۱-۳-۲- حملات لایه پیوند داده ۳۶

۲-۲- شبکه‌های پتری ۳۸
۲-۲-۱- تعریف رسمی از شبکه پتری پایه و خصوصیات آن ۳۹
۲-۲-۲- مشخصه‌های ساختاری شبکه‌های پتری ۴۰
۲-۲-۳- شبکه‌های پتری تصادفی و تصادفی تعمیم یافته ۴۵
۲-۲-۴- ارزیابی یک شبکه پتری تصادفی تعمیم یافته ۵۰
۲-۲-۵- شبکه‌های تصادفی مبتنی بر پاداش ۵۲
۲-۲-۶- شبکه‌های پتری فازی ۵۳
۲-۲-۶-۱- انواع عناصر فازی در شبکه پتری فازی ۵۴
فصل ۳- پژوهش‌های پیشین ۵۷
۳-۱- ارائه مدل تحلیلی جهت ارزیابی لایه پیوند داده: ۵۸
۳-۲- ارائه مدل تحلیلی جهت ارزیابی لایه شبکه: ۶۶
۳-۳- ارائه مدل تحلیلی برای دیگر جنبه‌های شبکه‌های موردی سیار ۶۸
فصل ۴- روش تحقیق ۷۳
۴-۱- مدل ارائه شده جهت لایه انتقال داده ۷۴
۴-۱-۱- مدل SRN جزئی هر گره ۷۶
۴-۱-۲- مدل برهم‌کنش گره‌ها ۸۲
۴-۱-۳- استخراج پارامترهای مرتبط با مدل ۸۷
۴-۱-۴- روابط لازم جهت محاسبه تعداد گره در یک فضای همسایگی ۹۰
۴-۱-۵- روابط لازم جهت محاسبه تعداد گره در ناحیه مخفی ۹۲

۴-۱-۶- پیاده‌سازی مدل اعمال حملات ۹۵
۴-۲- توصیف مدل لایه شبکه ۹۷
۴-۲-۱- مدل SRN برای فرآیند جریان داده‌ها ۹۸
۴-۲-۱-۱- محاسبه تعداد متوسط گام پیموده شده برای رسیدن بسته از مبدأ به مقصد ۱۰۵
۴-۲-۲- مدل SRN برای فرآیند مسیریابی ۱۰۹
۴-۳- ارائه پروتکل مسیریابی امن ۱۱۳
۴-۳-۱- تابع وارسی امنیت گره به گره ۱۱۴
۴-۳-۲- تابع وارسی امنیت مسیر ۱۲۰
۴-۳-۳- اصلاح پروتکل و پیاده‌سازی روش ۱۲۱
فصل ۵- پیاده‌سازی و ارزیابی ۱۲۷
۵-۱- تشریح سناریو استفاده شده ۱۲۹
۵-۲- ارزیابی لایه پیوند داده ۱۲۹
۵-۲-۱- حل مدل‌های SRN لایه پیوند داده ۱۳۰
۵-۲-۲- پیاده‌سازی و نتایج لایه پیوند داده ۱۳۱
۵-۲-۳- ارزیابی پیچیدگی زمانی جهت استخراج معیارهای کارایی ۱۴۳
۵-۲-۴- ارزیابی مقایسه ای با کارهای پیشین ۱۴۴
۵-۳- ارزیابی لایه شبکه ۱۴۸
۵-۴- ارزیابی مدل شبکه پتری فازی ارائه شده ۱۵۳
فصل ۶- نتیجه‌گیری و پیشنهاد کارهای آتی.....۱۵۹

۶-۱- بررسی لایه پیوند داده ۱۶۰
۶-۲- بررسی لایه شبکه..... ۱۶۲
۶-۳- بررسی مسیریابی امن مبتنی بر شبکه پتری فازی..... ۱۶۴
۶-۴- محدودیت‌های تحقیق و راهبرد آینده..... ۱۶۵
فهرست منابع ۱۶۷

فهرست شکل‌ها

شکل ۲-۱ نمونه‌ای از یک شبکه موردی سیار متشکل از چند گره بی‌سیم با انواع مختلف.....۱۱

شکل ۲-۲ پشته پروتکلی در شبکه‌های موردی سیار ۱۴

شکل ۲-۳ فرآیند کلی مسیریابی پروتکل DSR ۱۹

شکل ۲-۴ عملکرد کلی پروتکل مسیریابی AODV ۲۳

شکل ۲-۵ ساختار بسته‌های RREQ و RREP و جدول مسیریابی در پروتکل AODV ۲۴

شکل ۲-۶- نحوه عملکرد حمله Black-Hole ۲۷

شکل ۲-۷ فضای همسایگی بین چند گره در ارسال داده از طرف گره A به B به همراه محدوده‌های رادیویی مورد استفاده ۳۰

شکل ۲-۸ فلوچارت عملکرد پروتکل IEEE 802.11 DCF به ازای مکانیزم دست تکانی چهار مرحله‌ای RTS/CTS ۳۵

شکل ۲-۹ عملکرد گره‌ها در تنظیم مقدار تایمر NAV ۳۶

شکل ۲-۱۰: مثالی از ساختار شبکه پتری ۴۰

شکل ۳-۱ مدل مارکوف دوبعدی ارائه شده در مرجع [۳۷] به‌منظور نمایش مراحل مکانیزم انتظار تعویق ۵۹

شکل ۳-۲مدل SRN ارائه شده در مرجع [۴۶] جهت ارزیابی عملکرد پروتکل IEEE 802.11 DCF ۶۴

شکل ۳-۳ مدل SPN ارائه شده در مرجع [۵۰] جهت ارزیابی لایه شبکه ۶۷

شکل ۳-۴ مدل مارکوف پیوسته استفاده شده در مرجع [۵۶] جهت محاسبه میزان در دسترس بودن مسیر ۶۹

شکل ۴-۱ مدل SRN جزئی گره ۷۸

شکل ۴-۲ مدل SRN برهم‌کنش گره‌ها در لایه پیوند داده ۸۴

شکل ۴-۳: مدل SRN برای فرآیند جریان داده‌ها ۱۰۱

شکل ۴-۴: نرخ ترافیک داده اولیه (λ) از گره مبدأ تولید می‌شود که این نرخ در مقدار نسبت تحویل داده هر گره در طول مسیر از مبدأ تا مقصد ضرب می‌شود. ۱۰۵

شکل ۴-۵ فاصله اقلیدسی ارسال داده از گره مبدأ S به گره مقصد D با استفاده از گره میانی حائل M ۱۰۶

شکل ۴-۶: مدل SRN فرآیند مسیریابی بر اساس پروتکل AODV ۱۱۱

شکل ۴-۷. یک شبکه فرضی موردی سیار - مدل شبکه پتری فازی معادل شبکه ۱۱۵

شکل ۴-۸. چهار متغیر فازی برای فعال شدن اتصال ارتباطی (گذار) بین دو گره فعال هستند ۱۱۷

شکل ۴-۹ تابع عضویت فازی برای متغیر فازی، درصد بسته‌های داده منهدم شده ۱۱۸

شکل ۴-۱۰ تابع عضویت فازی برای متغیر فازی، نسبت تعداد RREQ های ۱۱۸

شکل ۴-۱۱. تابع عضویت فازی برای متغیر فازی، نسبت تعداد RREP های ارسالی به ۱۱۸

شکل ۴-۱۲ تابع عضویت فازی برای متغیر فازی، درصد به‌روزرسانی‌های غیرمعمول ۱۱۸

شکل ۴-۱۳ تابع عضویت فازی برای متغیر فازی، خروجی ۱۱۹

شکل ۴-۱۴: گره‌های P_1 و P_3 از طریق فعال نشدن انتقال مربوطه، برای ارسال و دریافت بسته از P_2 اجتناب می‌کنند ۱۲۱

شکل ۴-۱۵. قالب جدول همسایگی ایجاد شده شامل شناسه گره‌های همسایه و متغیرهای فازی مورداستفاده. ۱۲۳

شکل ۴-۱۶. قالب جدید الف) جدول مسیریابی و بسته‌های کنترلی ب) RREQ و ج) RREP در پروتکل اصلاحی ۱۲۴

شکل ۴-۱۷. مثالی از نحوه کارکرد پروتکل اصلاحی مبتنی بر شبکه پتری فازی ارائه شده ۱۲۵

شکل ۵-۱ نتایج به دست آمده به ازای معیارهای الف) توان گذردهی ب) تأخیر گام‌به‌گام برای ارزیابی پروتکل IEEE 802.11 DCF در مقابل اعمال چهار استراتژی حمله در لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۳۰۰ کیلوبایت بر ثانیه ۱۳۵

شکل ۵-۲ نتایج به دست آمده به ازای معیارهای الف) توان گذردهی ب) تأخیر گام‌به‌گام برای ارزیابی پروتکل IEEE 802.11 DCF در مقابل اعمال چهار استراتژی حمله در لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۶۰۰ کیلوبایت بر ثانیه ۱۳۶

شکل ۵-۳ نتایج به دست آمده به ازای معیارهای الف) توان گذردهی ب) تأخیر گام‌به‌گام برای ارزیابی پروتکل IEEE 802.11 DCF در مقابل اعمال چهار استراتژی حمله در لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۱ مگابایت بر ثانیه ۱۳۷

شکل ۵-۴ درصد استفاده از کانال برای گره‌های مشروع و متخاصم و درصد آزاد بودن برای حملات مختلف لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۳۰۰ کیلوبایت بر ثانیه ۱۳۸

شکل ۵-۵ درصد استفاده از کانال برای گره‌های مشروع و متخاصم و درصد آزاد بودن برای حملات مختلف لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۷۰۰ کیلوبایت بر ثانیه ۱۳۹

شکل ۵-۶ درصد استفاده از کانال برای گره‌های مشروع و متخاصم و درصد آزاد بودن برای حملات مختلف لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۱ مگابایت بر ثانیه ۱۴۰

شکل ۵-۷ نتایج به دست آمده از اعمال حملات ترکیبی در لایه پیوند داده برای معیار توان گذردهی با تنظیم نرخ تولید داده به مقدار ۳۰۰ کیلوبایت بر ثانیه.....۱۴۱

شکل ۵-۸ نتایج به دست آمده از اعمال حملات ترکیبی در لایه پیوند داده برای معیار توان گذردهی با تنظیم نرخ تولید داده به مقدار ۷۰۰ کیلوبایت ۱۴۲

شکل ۵-۹ نتایج به دست آمده از اعمال حملات ترکیبی در لایه پیوند داده برای معیار توان گذردهی با تنظیم نرخ تولید داده به مقدار ۱ مگابایت.....۱۴۲

شکل ۵-۱۰ : مقایسه مقادیر بدست آمده برای معیار توان گذردهی از مرجع [۳۸] و مدل ارائه شده در این تحقیق ۱۴۶

شکل ۵-۱۱ : مقایسه مقادیر بدست آمده برای معیار نسبت توان گذردهای گره های متخاصم توان گذردهی از مرجع [۳۹] و مدل ارائه شده در این تحقیق.....۱۴۸

شکل ۵-۱۲ ارزیابی نرخ تحویل بسته در لایه شبکه به ازای تعداد گره‌های موجود در اثر اعمال سه سطح از حملات الف) انهدام بسته ب) سیاه‌چاله ۱۵۱

شکل ۵-۱۳ تأخیر انتها به انتها در تحویل بسته در لایه شبکه به ازای تعداد گره‌های موجود در اثر اعمال سه سطح از حملات الف) انهدام بسته ب) سیاه‌چاله ۱۵۳

شکل ۵-۱۴ نسبت تحویل بسته برای تمام سطوح آستانه امنیتی در پروتکل امن مبتنی بر شبکه پتری فازی و AODV اصلی در مقابل تعدادی از گره‌های متخاصم. ۱۵۵

شکل ۵-۱۵ متوسط سطح امنیت برای تمام سطوح آستانه امنیتی در پروتکل امن مبتنی بر شبکه پتری فازی و AODV اصلی در مقابل تعدادی از گره‌های متخاصم. ۱۵۶

شکل ۵-۱۶: نتایج معیار PTDN برای تمام سطوح آستانه امنیتی در پروتکل امن مبتنی بر شبکه پتری فازی در مقابل تعدادی از گره‌های متخاصم. ۱۵۷

شکل ۵-۱۷: نتایج معیار PFDN برای تمام سطوح آستانه امنیتی در پروتکل امن مبتنی بر شبکه پتری فازی در مقابل تعدادی از گره‌های متخاصم.....۱۵۷

فهرست جدول‌ها

جدول ۴-۱ لیست گذارهای زمان‌دار و آنی استفاده شده در مدل جزئی گره‌ها ۸۳

جدول ۴-۲ توابع نگهبان مورداستفاده در مدل SRN شکل ۵-۲ .....۸۹

جدول ۴-۳ توابع نگهبان مورداستفاده در مدل SRN شکل ۵-۲ .....۸۹

جدول ۴-۴: قوانین فازی اعمال‌شده روی هر اتصال ارتباطی در تابع وارسی امنیت گره به گره ۱۲۲

جدول ۵-۱: نتایج مربوطه به پیچیدگی زمانی اجرای مربوط به محیط شبیه ساز NS-2 و استخراج نتایج از مدل ...۱۴۶

فصل ۱– مقدمه

۱-۱- توضیحات موضوع و ضرورت انجام آن

شبکه‌های موردی سیار[1] حاوی مجموعه‌ای از گره‌های[2] بی‌سیم مرتبط هستند که می‌توانند آزادانه و بدون داشتن هیچ‌گونه زیرساخت شبکه‌ای از پیش تعریف شده‌ای به‌صورت موردی ایجاد شوند. این شبکه‌ها به دلیل خصوصیات خود نظیر سرعت در برپایی، عدم نیاز به ساختار ارتباطی مشخص، سادگی در نصب و راه‌اندازی، هزینه‌های ارتباطی پایین و انعطاف و راحتی حاصل از ساختار پویای آن‌ها، نقش بسیار مهمی را در زمینه‌های مختلف خصوصاً کاربردهای نظامی و اضطراری ایفا می‌کنند. به همین علت‌ها نیز این شبکه‌ها در بسیاری از کاربردهای ارتباطی و شبکه‌ای جذاب به نظر می‌رسند [۱].

موارد استفاده این شبکه‌ها اغلب به‌گونه‌ای است که نیازمند عملکرد امن و مطمئن شبکه است و داشتن کارایی و امنیت بالا هدف مهمی در طراحی این شبکه‌ها می‌باشد [۲]. آن چیزی که بیشترین آسیب‌پذیری را به امنیت و کارایی شبکه‌های موردی سیار وارد می‌کند، حملاتی است که به این شبکه‌ها وارد می‌شوند. تحرک گره‌ها، بی‌سیم بودن ارتباطات، تغییر پویای ساختار شبکه، فقدان مدیریت متمرکز برای بررسی رفتارها و عملکردها، فقدان خطوط دفاعی مشخص و محدودیت در توان مصرفی گره‌ها، بستر مناسبی را برای حملات مختلف علیه این شبکه‌ها فراهم آورده است. لذا، مبحث امنیت در این شبکه‌ها امروزه یکی از مباحث مهم تحقیقاتی به شمار می‌رود [۳،۴].

با توجه به کاربرد وسیع و رو به رشد این نوع از شبکه‌ها در زمینه‌های مختلف ارزیابی کارایی آن بیش‌ازپیش ضروری به نظر می‌رسد. این ارزیابی البته دارای چالش‌های خاص خود می‌باشد. کارایی این شبکه‌ها تابع فاکتورهای زیادی ازجمله میزان بار ترافیک ورودی، تعداد گره‌ها، اندازه شبکه، نرخ خرابی و بازیابی اتصالات، مدل حرکتی گره‌ها و ارتباط میان گره‌ها در لایه‌های مختلف و همچنین

---

[1] ad-hoc network
[2] nodes

تأثیر گره‌های مخربی می‌باشد که به‌نوعی سعی می‌کنند عملکرد این شبکه را با قصد خودخواهانه[1] و یا خصمانه[2] مختل کنند [۸].

به‌منظور ارزیابی کارایی شبکه‌های موردی سیار در اکثر تحقیقات صورت گرفته از شبیه‌سازهای گسسته رخداد مانند NS-2، Glomosim، OPNET و مانند آن استفاده می‌کنند. در این رویکرد تلاش می‌شود تا عملکرد پروتکل‌های شبکه در لایه‌های مختلف را با نوشتن کدهای مربوطه در یک فضای کامپیوتری شبیه‌سازی کرد. در این حالت می‌توان رفتار سیستم را تحت شرایط متفاوت بررسی کرده و به درکی از رفتار آن در دنیای واقعی رسید. در این نوع از شبیه‌سازها، مشخصه‌های کاربردی سیستم که معرف حالت جاری آن هستند در بازه‌های زمانی گسسته اندازه‌گیری شده و در پایان شبیه‌سازی به‌صورت داده‌های خام در اختیار پایانه کاربر قرار می‌گیرد با وجود فراگیر بودن استفاده از این نوع از شبیه‌سازها ارزیابی کارایی توسط آن اغلب دارای چالش‌های خاص خود می‌باشد [۵].

نتایج به دست آمده از این شبیه‌سازها تنها برای مقادیر خاصی از پارامترها صحیح است. به‌عنوان‌مثال فرض کنید که هدف آن است که توسط یک شبیه‌ساز، نرخ تحویل بسته را بر اساس یک اندازه بعد از مساحت صفحه‌ای که گره‌ها در آن حرکت می‌کنند به دست آورده شود. واضح است که مقدار به دست آمده تنها برای آن مقدار از ابعاد صفحه صحیح است و اگر ابعاد صفحه تغییر کند مقدار نرخ تحویل بسته نیز تغییر خواهد کرد. درصورتی‌که خواسته شود به قانونی از نسبت اندازه صفحه و نرخ تحویل بسته برسیم لازم است که این آزمایش چندین مرتبه به ازای مقادیر مختلف تکرار شود که این کار زمان و منابع زیادی را صرف می‌کند. در بسیاری از موارد نتایج به دست آمده از یک شبیه‌سازی در شبیه‌سازهای دیگر و یا در اجراهای دیگر از همان شبیه‌ساز باهم متفاوت است که این مشکلی دیگر در

---

[1] Selfishly
[2] Misbehaviorly

کار با شبیه‌ساز است که گزارش‌های آن در مراجع [۶ و ۷ و ۸] آورده شده است. بر اساس آنچه در مرجع [۶] ذکر شده برای حصول یک نتیجه یکسان از شبیه‌سازهای مختلف لازم است تا یک سناریو مشخص را حداقل ۵ بار اجرا کرده و از نتایج به دست آمده میانگین‌گیری شود. در این صورت نتایج تا حدودی یکسان خواهد بود. همچنین در مراجع [۹ و ۸] با شبیه‌سازی یک سناریو واقعی نشان داده شده که مقادیر به دست آمده از شبیه‌ساز NS-2 بیشتر به واقعیت نزدیک‌تر است.

در رویکرد دیگری از ارزیابی شبکه‌های موردی سیار می‌توان از مدل‌سازی تحلیلی و یا تکنیک‌های تحلیل ریاضی استفاده نمود. در مدل‌سازی تحلیلی، رفتار سیستم تحت قالب روابط منطقی، بصورت بصری و درنهایت با استفاده از معادلات ریاضی نشان داده می‌شود. این امر بیانگر نحوه عکس‌العمل سیستم به ازای مقادیر پارامتر متفاوت است. در بسیاری از موارد به دست آوردن این روابط ریاضی کاری دشوار است و ابزارهای مدل‌سازی تحلیلی مانند شبکه‌های پتری و یا زنجیره های مارکوف با مدل‌سازی عملکرد شبکه در غالب روابط آماری ما را در رسیدن به آن کمک می‌کنند. استفاده از این روش علاوه بر این، امکان یک دید بصری را از نحوه عملکرد سیستم مورد مطالعه فراهم می‌کند که می‌تواند در ارزیابی آن توسط تحلیلگر نقش بسزایی داشته باشد. این امکان، دقیقاً برخلاف آن چیزی است که در غالب شبیه سازهای گسسته رخداد وجود دارد که در آن تحلیلگر مجبور به مطالعه و جستجو در کدهای پیچیده ارائه شده برای یک الگوریتم جهت آزمودن آن است.

۱-۲- اهداف و روش

همان‌طور که در بالا ذکر شد استفاده از مدل‌سازی تحلیلی به‌جای محیط‌های شبیه‌سازی در تحلیل کارایی این شبکه‌ها سبب کاهش زمان اجرای فرآیند و دستیابی به یک ارزیابی دقیق و جامع با پشتوانه ریاضی از آن و همچنین امکان ارائه یک دید بصری از سیستم مورد مطالعه خواهد شد. استفاده از نتایج این ارزیابی در طراحی پروتکل‌های مسیریابی می‌تواند سبب پیدا کردن چالش‌های امنیتی در طراحی آن و امکان آزمودن آسان راهبردهای امنیتی مختلف جهت بهبود آن شود.

مدل‌سازی سیستم‌ها معمولاً توسط ابزارهای متفاوتی انجام می‌شود. ازجمله آن می‌توان به تکنیک‌های مدل‌سازی تحلیلی مانند شبکه‌های پتری، ماکس الجبرا و مدل‌های مارکوف اشاره کرد که به‌منظور ارزیابی عملکرد شبکه‌های ارتباطی استفاده می‌شوند. کارایی این ابزارها در جهاتی با هم متفاوت هستند. بعضی تنها یک شمای گرافیکی از سیستم را ارائه می‌دهند و بعضی نیز تا حد ارائه اثبات‌های ریاضی از مدل ایجادشده پیش می‌روند.

شبکه‌های پتری به‌عنوان یک ابزار قدرتمند تحلیلی و زبان توصیفی سطح بالا برای مدل‌سازی سیستم‌های پیچیده گسسته رخداد که در حوزه وسیعی از کاربردهای مهندسی مطرح می‌باشد، نمونه بارزی از روش‌های مدل‌سازی تحلیلی است. شبکه‌های پتری علاوه بر دارا بودن امکانات لازم جهت مدل‌سازی هر نوع از سیستم، دارای خصوصیاتی جهت ارزیابی و وارسی کردن سیستم مورد بحث نیز می‌باشد. لذا در این تحقیق اقدام به ارزیابی عملکرد شبکه‌های موردی سیار در دو لایه شبکه و پیوند داده در مقابل حملات مرسوم وارده به آن شده است. مدل‌سازی فرآیند کار با استفاده از کلاسی از شبکه‌های پتری به نام شبکه تصادفی مبتنی بر پاداش[1] صورت گرفته که نوع کامل‌تری از شبکه‌های پتری تصادفی تعمیم‌یافته[2] می‌باشد. در انجام فرآیند تحقیق فرض می‌شود که در لایه شبکه از الگوریتم مسیریابی AODV و همچنین در لایه پیوند داده از پروتکل IEEE 802.11 DCF استفاده شده است. ارزیابی درستی مدل ارائه شده با استفاده روش ارزیابی مقایسه‌ای با تعریف یک سناریو در محیط شبیه‌ساز و ترجمه آن در مدل ارائه شده و استخراج نتایج جهت بررسی میزان تطابق دو محیط صورت می‌گیرد.

---

[1] Stochastic Reward Net
[2] Generlized Stochastic Petri net

۱-۳- فرضیات تحقیق

در انجام این تحیق فرضیات ذیل محفوظ می باشد

- استفاده از الگوریتم مسیریابی AODV در لایه شبکه
- استفاده از پروتکل IEEE 802.11 DCF در لایه پیوند داده
- بررسی تنها حملات مسیریابی در لایه شبکه
- یکسان بودن نرخ ارسال داده گره‌های متخاصم و مشروع
- هیچ فرضی در ارتباط با مکان گره‌های متخاصم و مشروع وجود ندارد
- استفاده از مدل حرکتی Random Way Point برای گره‌های متخاصم و مشروع
- حرکت گره‌ها در یک فضای به شکل مربع

۱-۴- چالش‌ها

استفاده از روش‌های مدل‌سازی تحلیلی اغلب دارای پیچیدگی‌های متفاوتی است. نوعی از پیچیدگی آن ناشی از ماهیت تحلیلی/نظری روش بکار گرفته‌شده می‌باشد. به‌عبارت‌دیگر روش‌های تحلیلی موجود خود دارای پیچیدگی‌های نظری می‌باشند که کاربرد آن‌ها مستلزم دقت و آگاهی کامل از ماهیت ریاضی روش مورداستفاده می‌باشد. استفاده از این روش در تحلیل خصوصیات یک سیستم و به‌طور خاص شبکه‌ها اغلب نیازمند تقریب جنبه‌های رفتاری گره‌ها در یک فضای احتمالاتی است. به عنوان مثال در ارتباط با موضوع تحقیق پیش رو، لازم است تا احتمال مواردی چون آزاد بودن کانال در یک فضای همسایگی و یا احتمال رسیدن یک بسته به مقصد را حساب کنیم که اغلب دارای پیچیدگی‌های زیادی هستند. همچنین این سیستم‌ها معمولاً شامل یکسری فرآیندهای موازی[1]

[1] Concurrent

هستند و بالطبع آن نیازمند مکانیزم های پیچیده سنکرون‌سازی[1] برای دستیابی به این منابع می‌باشند. رفتار هر مؤلفه در این سیستم‌ها هم تابع فرآیندهای داخلی و هم تابع فرایندهای کل سیستم است. به‌عنوان‌مثال در مدل‌سازی شبکه، رفتاری که یک گره در شبکه از خود بروز می‌دهد تنها وابسته به گره‌های همسایه با فاصله یک گام[2] از آن نیست، بلکه به رفتار گره‌های دیگر شبکه که جدا از آن هستند نیز وابسته است. یا رفتارهای موازی گروهی از گره‌ها و نحوه تعامل این گره‌ها با یکدیگر به‌صورت مدول های مستقل موازی مدل‌سازی چالش‌های ابزاری را ایجاد می‌کند.

همچنین در ارائه یک سیستم توسط مدل‌ها، هر گام رفتاری سیستم توسط یک وضعیت[3] نشان داده می‌شود. در مواردی، تعداد این وضعیت‌ها آن‌قدر زیاد می‌شود که تحلیل آن برای ابزار آزمودن مدل مشکل خواهد بود که به این پدیده انفجار حالت‌ها[4] گفته می‌شود. در این حالت تحلیل سیستم با خطا مواجه می‌شود، نه به خاطر وجود خطا در سیستم بلکه به خاطر نبود حافظه کافی در سیستم مقصد جهت انجام آن. درواقع طراحان مدل لازم است تا از طرفی به فکر کاهش پیچیدگی زمانی سیستم از طریق کم کردن تعداد حالت‌ها باشند. درعین‌حال نیز باید رفتارها و مشخصه‌های اساسی سیستم را توسط وضعیت‌ها نشان دهند. در طراحی عملکرد شبکه‌های موردی سیار با استفاده از شبکه‌های پتری لازم است راهبرد مناسب جهت رفع این مشکل ارائه شود. قطعاً داشتن نگاهی با سطح انتزاع بالاتر به عملکرد پروتکل مسیریابی سبب کاهش تعداد حالت‌های مدل شبکه پتری و تا حدودی رفع این مشکل خواهد شد. اما این کار موجب عدم توجه به بعضی جزئیات عملکردی و در نهایت تفاوت مقادیر حاصل از مدل شبکه پتری با پیاده‌سازی‌های دیگر خواهد شد.. ارائه یک مدل خوب از سیستم درواقع

---

[1] Synchronaziation
[2] one-hop communication
[3] State
[4] State Space explosion

حد تعادلی بین کاهش تعداد وضعیت‌های سیستم به‌منظور جلوگیری از مشکل انفجار حالت‌ها و نشان دادن رفتار جزئی و دقیق سیستم توسط این وضعیت‌های می‌باشد

در ادامه نوشتار، در فصل ۲ به بررسی ادبیات تحقیق خواهیم پرداخت که در آن تعریف جامعی از شبکه‌های موردی سیار و ساختار پروتکل‌های آن خصوصاً در دولایه پیوند داده و شبکه ارائه خواهد شد. همچنین به ارائه توضیحات لازم در خصوص شبکه‌های پتری و انواع آن با تمرکز روی مدل‌های پتری تصادفی در این فصل اقدام شده است. روش‌های تحلیل و ارزیابی و استخراج پارامترهای ارزیابی از یک مدل پتری تصادفی به‌تفصیل در این فصل توضیح داده شده است. در فصل ۳ نیز کارهای پیشین صورت گرفته در موضوع تحقیق مورد بررسی قرار گرفته است. با توجه به کمبود کارهای صورت گرفته در این خصوص، مطالعات انجام شده با استفاده از روش‌هایی مانند مارکوف و روابط ریاضی نیز در این بخش بررسی شده‌اند. در فصل ۴ نیز روش ارائه شده برای تحقیق تشریح شده است. که دارای سه بخش کلی مدل‌سازی لایه پیوند داده با استفاده از شبکه پتری نوع SRN، مدل‌سازی لایه شبکه و حملات آن با استفاده از SRN و درنهایت ارائه یک پروتکل مسیریابی امن بر مبنای شبکه پتری فازی. فصل ۵ نیز حاوی آزمایش‌ها صورت گرفته در حیطه روش‌های ارائه شده در فصل ۴ براساس تعداد گره‌های شبکه، نرخ ترافیک ارسال داده و پارامترهای دیگر می‌باشد. در فصل ۶ نیز نتیجه گیری کوتاهی از تحقیق انجام شده، محدودیت های آن و همچنین راهبرد آینده ارائه خواهد شد.

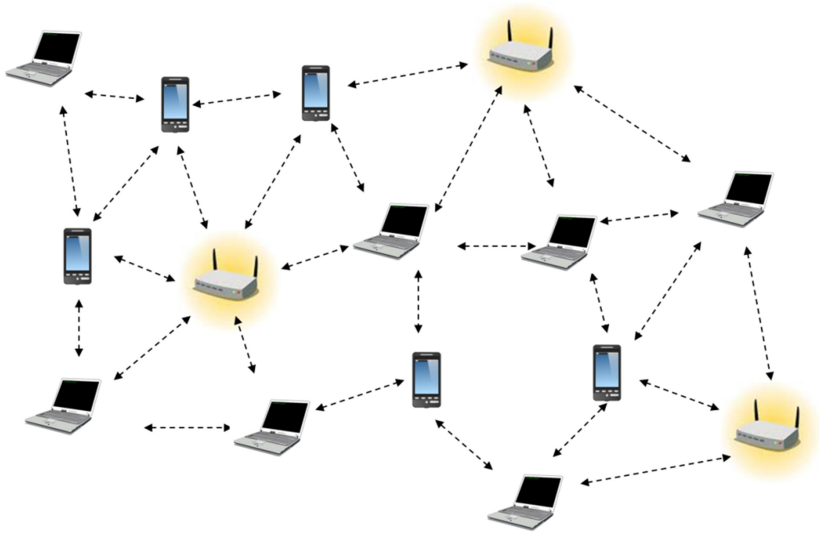
فصل ۲– ادبیات تحقیق

۲-۱- شبکه‌های موردی سیار

شبکه‌های موردی سیار[1] حاوی مجموعه‌ای از گره‌های[2] بی‌سیم مرتبط هستند که می‌توانند آزادانه و بدون داشتن هیچ‌گونه زیرساخت شبکه‌ای از پیش تعریف شده‌ای به‌صورت موردی ایجاد شوند. این شبکه‌ها به دلیل خصوصیات خود نظیر سرعت در برپایی، عدم نیاز به ساختار ارتباطی مشخص، سادگی در نصب و راه‌اندازی، هزینه‌های ارتباطی پایین و انعطاف و راحتی حاصل از ساختار پویای آن‌ها، نقش بسیار مهمی را در زمینه‌های مختلف خصوصاً کاربردهای نظامی و اضطراری ایفا می‌کنند. به همین علت‌ها نیز این شبکه‌ها در بسیاری از کاربردهای ارتباطی و شبکه‌ای جذاب به نظر می‌رسند [۱]. از موارد استفاده شبکه‌های موردی می‌توان به کاربردهای شخصی مانند اتصال رایانه‌های قابل‌حمل به یکدیگر، کاربردهای عمومی مانند ارتباط وسایل نقلیه و تاکسی‌ها، کاربردهای نظامی مانند ارتش و ارتباط ناوگان جنگی و کاربردهای اضطراری مانند عملیات امداد و نجات اشاره کرد. ارتباط میان گره‌ها در این شبکه از طریق امواج رادیویی صورت می‌گیرد. درصورتی‌که یک گره در محدوده رادیویی گره دیگر باشد همسایه آن گره به‌حساب می‌آید. در غیر این صورت در صورت نیاز به ارتباط میان دو گره که در محدوده رادیویی یکدیگر نیستند می‌توان از کمک گره‌های دیگر در این مورداستفاده کرد. بنابراین ارتباط میان گره‌ها در این شبکه به‌نوعی بر مبنای اعتماد و مشارکت میان گره‌ها صورت می‌گیرد. شکل ۲-۱ نمونه‌ای از یک شبکه موردی سیار را نشان می‌دهد.

---

[1] ad-hoc network
[2] nodes



شکل ۲-۱ نمونه‌ای از یک شبکه موردی سیار متشکل از چند گره بی‌سیم با انواع مختلف

۲-۱-۱-مشخصات شبکه‌های موردی سیار

شبکه‌های موردی سیار دارای یکسری مشخصه‌های منحصربه‌فردی هستند که آن‌ها را از دیگر شبکه‌های مرسوم سیمی متمایز می‌کند. وجود این مشخصه‌های خاص به‌نوعی سبب می‌شود تا بسیاری از عملیات صورت گرفته روی آن‌ها ازجمله طراحی پروتکل‌های مسیریابی و یا اعمال تدابیر امنیتی با شبکه‌های دیگر متفاوت باشد. این مشخصه‌ها اغلب به‌گونه‌ای هستند که اعمال کاربردهای مختلف را روی آن‌ها با چالش‌هایی بعضاً امنیتی مواجه می‌کنند. این موارد اغلب نقطه‌ضعفی برای این شبکه‌ها محسوب می‌شوند که البته در مقابل مزیت‌هایی مطرح‌شده در بالا قابل‌چشم‌پوشی و مدیریت می‌باشند [۱۰].

- **خودمختاری و تحرک گره‌ها**: هر گره در شبکه‌های موردی سیار به‌صورت خودمختار عمل می‌کند و نقش یک مسیریاب و میزبان را باهم ایفا می‌کند. هیچ ساختار متمرکزی برای گره‌ها در شبکه‌های موردی سیار وجود ندارد. این امر سبب می‌شود تا به‌عنوان‌مثال گره‌ها نتوانند به امکانات امنیتی شبکه اعتماد کنند و هر گره لازم است تا امنیت خود را در نظر داشته باشد. بنابراین طراحی پروتکل‌های مسیریابی و امنیتی را نمی‌توان در این نوع از شبکه‌ها به‌صورت

متمرکز انجام داد و کمترین میزان دخالت در ساختار این شبکه‌ها موردنیاز است. از طرف دیگر، تحرک گاه‌به‌گاه گره‌ها سبب تغییر پویای توپولوژی شبکه خواهد شد. گره‌های متحرک می‌توانند به‌آسانی به شبکه وارد یا از آن خارج شوند بدون اینکه هیچ‌گونه اعمال محدودیتی روی آن‌ها اعمال شود.

- **توزیع‌شدگی و مسیریابی پویای چندگامه**[1]: این شبکه‌ها در عملیاتشان مانند مسیریابی و امنیت به‌صورت توزیع‌شده عمل می‌کنند به‌عنوان‌مثال برخلاف شبکه‌های سیمی این شبکه‌ها نمی‌توانند دارای یک دیواره آتش[2] متمرکز باشد. گره‌ها به‌راحتی می‌توانند به شبکه وارد و یا از آن خارج شوند. بنابراین توپولوژی یا همبندی آن دینامیک است. همچنین، درصورتی‌که گره مبدأ و گره مقصد در محدوده رادیویی یکدیگر نباشند یک مسیریابی چندگامه مورد نیاز است
- **منابع محدود شبکه:** گره‌های موجود در این شبکه اغلب دارای ظرفیت حافظه و توان پردازشی و عمر باطری کمی برخوردار هستند. پایداری و ظرفیت و قابلیت اعتماد اتصال‌های ارتباطی در شبکه‌های بی‌سیم همواره نامرغوب‌تر از شبکه‌های سیمی است. به‌عنوان‌مثال کانال ارتباطی گره‌ها در این نوع از شبکه به‌گونه‌ای است که در آن تنها یک گره از یک فضای همسایگی امکان تصاحب کانال و انتقال داده در آن را دارد. این موارد سبب می‌شود تا نتوان الگوریتم‌های پیشرفته که منابع زیادی نیاز دارد را روی آن اعمال کنیم.
- **چالش‌های امنیتی:** موارد استفاده این شبکه‌ها اغلب به‌گونه‌ای است که نیازمند عملکرد امن و مطمئن شبکه است و داشتن کارایی و امنیت بالا هدف مهمی در طراحی این شبکه‌ها می‌باشد. آن چیزی که بیشترین آسیب‌پذیری را به امنیت و کارایی شبکه‌های موردی سیار وارد می‌کند، حملاتی است که به این شبکه‌ها اعمال می‌شوند. تحرک گره‌ها، بی‌سیم بودن ارتباطات، تغییر

---

[1] Distribution
[2] Firewall

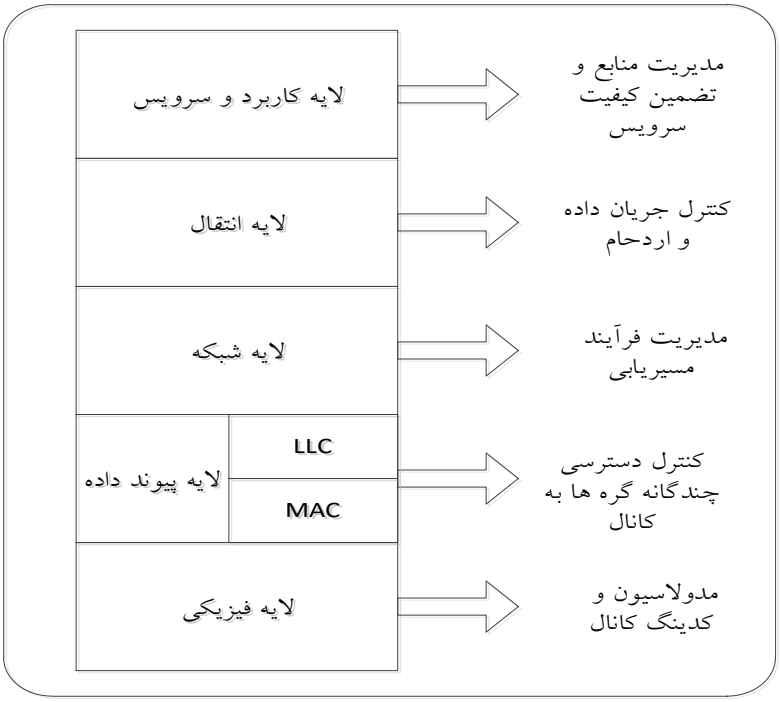
پویای ساختار شبکه، فقدان مدیریت متمرکز برای بررسی رفتارها و عملکردها، فقدان خطوط دفاعی مشخص و محدودیت در توان مصرفی گره‌ها، بستر مناسبی را برای حملات مختلف علیه این شبکه‌ها فراهم آورده است. به خاطر ساختار مسیریابی شبکه‌های موردی سیار که به‌نوعی بر مبنای نوعی اعتماد میان گره‌ها استوار است فرصت خوبی را برای حمله‌کنندگان فراهم می‌کند تا با شرکت در فرآیند مسیریابی به‌نوعی باعث فریب دادن فرآیند مسیریابی شده و نهایتاً امر مسیریابی را مختل کنند. خاصیت خود ساختاری[1] شبکه‌های موردی سیار نیز باعث به وجود آمدن یکسری از حملات خواهد شد. الگوریتم‌های مسیریابی که روی شبکه‌های موردی سیار عمل می‌کنند اغلب نیازمند اعتماد کامل میان گره‌ها هستند که این امر سبب کاهش ضریب امنیتی در این شبکه‌ها می‌شود. مکانیزم ساختاری این شبکه به نحوی است که با ورود یک گره لازم است تا با کسب اطلاعات از گره‌های دیگر اقدام به تخصیص آدرس IP به آن نمایند. یک گره خرابکار[2] می‌تواند در این امر اختلال ایجاد کند و یا آدرس IP گره اختصاص‌یافته را برای خود در نظر بگیرد. به همین دلیل استفاده از تکنیک‌های جلوگیری از حمله در این شبکه‌ها با محدودیت‌های بیشتری مواجه است. به‌عنوان‌مثال مکانیزم های رمزگذاری[3] و اعتبارسنجی[4] در این شبکه‌ها برای مقاصد دفاعی استفاده می‌شود. ولی با توجه به ساختار این شبکه‌ها این احتمال وجود دارد که یک گره دزدیده شود و در صورت وجود کلید اختصاصی[5] برای آن، این کلید لو برود. بنابراین این مکانیزم نیز بلااستفاده خواهد بود [۱۱،۱۲].

---

[1] Self-organization
[2] malicious node
[3] encryption
[4] authentication
[5] Private Key

۲-۱-۲-پشته پروتکلی در شبکه‌های موردی سیار

این بخش توضیح کوتاهی روی پشته پروتکل OSI شبکه‌های موردی سیار ارائه می‌کند. ساختار پشته پروتکلی در شکل ۲-۲ برای شبکه‌های بی‌سیم نمایش داده شده که بسیار شبیه به ساختار پشته پروتکلی در شبکه‌های مرسوم سیمی است[۱۳]. در اینجا نیز به‌منظور استقلال عملیات صورت گرفته در شبکه و امکان توسعه راحت‌تر آن در آینده از یک ساختار لایه‌ای به‌منظور نمایش آن استفاده شده است. هر لایه می‌تواند مطابق با یکی از استانداردهای مرسوم موجود برای شبکه‌های بی‌سیم کار کند. اولین لایه، لایه کاربرد و ارائه سرویس می‌باشد که بالای پشته را اشغال می‌کند. لایه‌های انتقال، شبکه، پیوند داده و فیزیکی در زیر قرار می‌گیرند. لایه کاربرد و ارائه سرویس وظایفی مانند تقسیم و تعادل کار بین گره‌های ثابت و متحرک و همچنین مدیریت توان مصرفی گره‌ها و تضمین کیفیت سرویس ارائه شده را بر عهده دارد. سایر لایه‌ها در این پشته پروتکل در ادامه توضیح داده شده است.



شکل ۲-۲ پشته پروتکلی در شبکه‌های موردی سیار

لایه فیزیکی: عملیات و سرویس‌های عمده‌ای که توسط لایه فیزیکی در شبکه‌های موردی سیار انجام می‌گیرد شامل رمزگذاری، مدولاسیون، انتقال، دریافت و رمزگشایی می‌باشد. استاندارد IEEE 802.11 سه فناوری فیزیکی را پشتیبانی می‌کند که عبارت است از: DSSS[1], FHSS[2], DFIR[3]. فناوری DSSS از فرکانس رادیویی در محدوده ۲,۴ تا ۲,۴۸۳۵ (گیگاهرتز) عمل کرده و از مدولاسیون نوع DBPSK[4],DQPSK[5] استفاده می‌کند. FHSS در همان محدوده فرکانسی مشابه DSSS و پهنای باند ۸۳,۵ مگاهرتز استفاده می‌کند. این فناوری از FSK[6] دو و چهار سطحی استفاده می‌کند. و کل پهنای باند را به ۷۹ کانال ۱ مگاهرتزی تقسیم می‌کند. DFIR فقط برای مصرف داخلی است. و از تکنیک مدولاسیون از PPM[7] استفاده می‌کند [۱۵ و ۱۴].

لایه پیوند داده: این لایه به دو زیرلایه به نام‌های LLC و MAC تقسیم می‌گردد. LLC درواقع همانند یک لایه مجازی روی لایه MAC قرار گرفته و امکان ترجمه و ارتباط بین پروتکل‌های مختلف لایه MAC را فراهم می‌کند. یک پروتکل لایه MAC در شبکه‌های بی‌سیم مشخص می‌کند که چگونه گره‌ها ارتباطشان را روی کانال عمومی که در یک فضای همسایگی از گره وجود دارد هماهنگ کنند. همچنین یک پروتکل در این لایه لازم است تا امکان یک ارتباط پایدار، منصفانه و کارآمد را برای ارتباط گره‌ها فراهم کند. وظایف یک پروتکل در لایه MAC شامل آدرس‌دهی واحدهای انتقال داده، تخصیص کانال، قالب‌بندی قطعات[8]، بررسی خطا، قطعه‌قطعه کردن بسته داده و سرهم‌بندی آن در

[1] Direct Sequence Spread Spectrum
[2] Frequency Hopping Spread Spectrum
[3] Diffused Infrared
[4] Differential Binary Phase Shift Keying
[5] Differential Quadruple Phase Shift Keying
[6] Frequency Shift Keying
[7] Pulse Position Modulation
[8] Frame Formatting

دریافت است. همچنین حل مشکلاتی مانند گره پنهان[1] و گره آشکار[2] نیز برعهده یک پروتکل در این لایه می‌باشد [۱۶،۱۵].

لایه شبکه: پروتکل‌های مسیریابی این شبکه‌ها به علت به‌روزرسانی زیاد مسیرها، تحرک گره‌ها و محدودیت محدوده ارتباطی با آنچه در شبکه‌های سیمی وجود دارد متفاوت است. لذا پروتکل مسیریابی‌مورد استفاده در آن لازم است تا موارد زیر را در نظر داشته باشد [۱۷].

- با توجه به اینکه مسیریابی متمرکز شامل سربار زیادی است و درنتیجه مقیاس‌پذیر نمی‌باشد لذا لازم است تا الگوریتم مسیریابی آن کاملاً توزیع‌شده باشد
- باید نسبت به تغییر زیاد توپولوژی شبکه که به علت حرکت زیاد گره‌ها رخ می‌دهد سازگار باشد.
- محاسبه و نگهداری مسیرها باید شامل حداقل تعداد مسیرها باشد و گره‌های موجود لازم است تا سریع‌ترین دسترسی را به مسیرها داشته باشند.

تقسیم‌بندی عمده‌ای که در مورد پروتکل‌های مسیریابی شبکه‌های موردی سیار وجود دارد شامل پروتکل‌های واکنشی، پروتکل‌های پیش کنشی و پروتکل‌های ترکیبی می‌باشد.

لایه انتقال: لایه انتقال یک سرویس ارتباط انتها به انتها را برای لایه کاربردی فراهم می‌کند. این سرویس اغلب شامل کنترل خطا، کنترل جریان، کنترل ازدحام و تسهیم می‌باشد. دو پروتکل رایج لایه انتقال TCP و UDP است. UDP یک پروتکل بدون اتصال در لایه انتقال است که UDP به دلیل فراهم نکردن کنترل جریان یا کنترل خطا یک پروتکل قابل‌اطمینان محسوب نمی‌شود و اساساً به‌عنوان یک واسط میان لایه شبکه و لایه کاربردی عمل می‌کند. در مقابل،TCP یک پروتکل انتقال

---

[1] Hidden node
[2] Exposed node

اتصال گرا است که برای اطمینان از رسیدن بسته به مقصد مورد نیاز است. برای استفاده مؤثر از پهنای باند شبکه و کنترل جریان بسته‌ها، TCP از یک مکانیسم شناخته‌شده با عنوان پنجره لغزان[1] استفاده می‌کند. این مکانیزم به فرستنده اجازه می‌دهد تا چندین بسته را قبل از منتظر ماندن برای دریافت یک ACK ارسال کند. استفاده از TCP در این شبکه‌ها خیلی مناسب به‌نظر نمی‌رسد. البته تلاش‌هایی در جهت بهینه ساختن عملکرد TCP و استفاده از آن در شبکه‌های بی‌سیم صورت گرفته است [۱۳ و ۱۴].

با توجه به مطالب گفته‌شده در بالا و بر اساس گزارش‌های ارائه شده در [۱۸ و ۱۹ و ۲۰] به این نتیجه می‌رسیم که عمده فعالیت انجام شده در ارتباط بین گره‌ها در یک شبکه بی‌سیم در لایه‌های پیوند داده و شبکه انجام می‌شود. به همین دلیل نیز عمده حملات موجود در این شبکه‌ها نیز در این دو لایه صورت می‌پذیرد. لذا، در ادامه به بررسی دقیق‌تر پروتکل‌های موجود در این دو لایه خواهیم پرداخت.

۲-۱-۲-۱- لایه شبکه در شبکه‌های موردی سیار

این بخش به بررسی پروتکل‌های موجود در لایه شبکه، شبکه‌های موردی سیار می‌پردازد که جهت مسیریابی یک بسته از مبدأ به مقصد از آن‌ها استفاده می‌شوند. پروتکل‌های این لایه به سه دسته عمومی پروتکل‌های واکنشی، پروتکل‌های پیش کنشی و پروتکل‌های ترکیبی تقسیم می‌شوند. در ادامه پروتکل‌های نمونه و شاخص در هریک از این دسته‌ها با ذکر جزئیات بیشتر بررسی خواهند شد.

[1] Sliding window

۲-۱-۲-۲-پروتکل‌های پیش کنشی

در پروتکل‌های از این نوع، گره‌ها مدام در حال جستجوی اطلاعات مسیریابی جدید درون شبکه هستند. بنحوی که حتی با تغییر مکان گره‌ها در صورت نیاز به‌راحتی می‌توان مسیر مناسبی را یافته و برای ارسال و دریافت اطلاعات بین هر دو گره استفاده کرد. به عبارت بهتر می‌توان گفت که در این شبکه‌ها مسیرها از قبل موجود هستند و به‌محض آنکه گره‌ای اقدام به ارسال داده به گره دیگری کند می‌تواند مسیر موجود را از روی اطلاعات از قبل جمع‌آوری‌شده شناسایی کرده و مورد استفاده قرار دهد. لذا گره‌ها در فرآیند مسیریابی خود دچار تأخیری نخواهند شد. الگوریتم های مسیریابی بردار فاصله مبتنی بر شماره توالی مقصد (DSDV) [۲۱] و یا مسیریابی مبتنی بر خوشه (CGSR) [۲۲] از جمله پروتکل‌های پیش‌کنشی هستند.

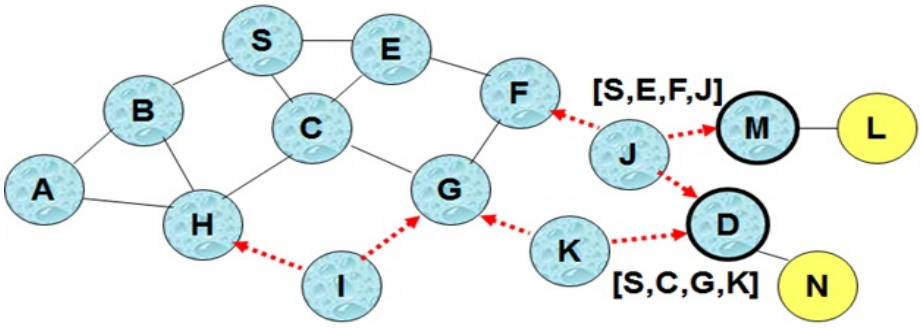
۲-۱-۲-۳-پروتکل‌های واکنشی

در این نوع پروتکل، مسیرها تنها زمانی کشف می‌شوند که مبدأ قصد برقراری ارتباط با گره دیگری در شبکه کند. زمانی که یک گره بخواهد با گره دیگری ارتباط برقرار کند لازم است تا فرآیند کشف مسیر[1] را در شبکه فراخوانی کند. در این نوع از پروتکل‌های مسیریابی، قبل از برقرار شدن ارتباط، تأخیر قابل‌توجهی مشاهده می‌شود. در این قسمت برخی از پروتکل‌های این دسته شرح داده خواهند شد:

مسیریابی پویای از مبدأ (DSR[2]). در این نوع از پروتکل مسیریابی از بسته‌های Rout Request(RREQ) و Rout Replay(RREP) به‌منظور کشف مسیر استفاده می‌شود. شیوه کار بدین‌صورت است که ابتدا گره مبدأ S که قصد ارسال داده به مقصد D را دارد اقدام به پخش همگانی بسته‌های RREQ می‌کند. همسایه‌های این گره با شنیدن آن درصورتی‌که مسیری به مقصد داشته

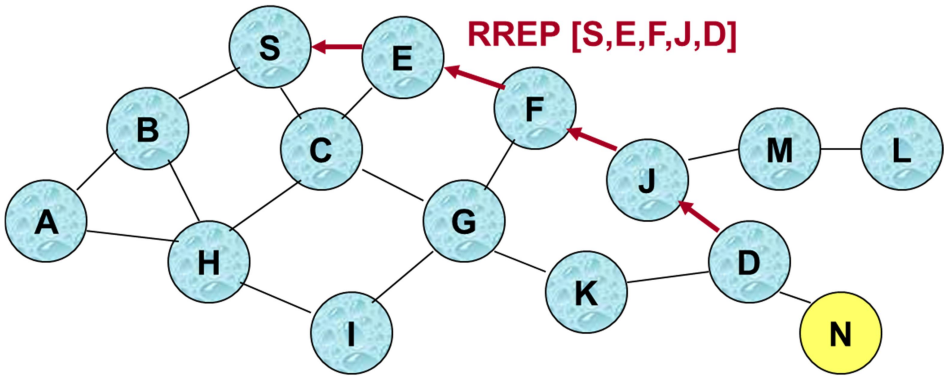
[1] Route Discovery Process
[2] Dynamic source routing

باشند با ارسال یک بسته RREP به آن پاسخ می‌دهند. در غیر این صورت با افزودن شناسه IP خود به آن فرآیند پخش همگانی به همسایگان را تا رسیدن به گره مقصد و یا گره‌ای که از آن اطلاع دارد ادامه می‌دهد. در این صورت، مسیر طی شده از گره مبدأ به آن در سرآیند نهایی بسته مشخص شده است و از طریق همان مسیر بسته RREP به گره مبدأ بازگشت داده می‌شود. در ادامه، گره مبدأ با دریافت RREP که حاوی آدرس تا گره مقصد است بسته داده را به سمت مقصد نهایی ارسال می‌کند. فرآیند کلی پروتکل مسیریابی DSR در شکل‌های ۲-۳ (الف، ب، ج) آمده است. در نوع بهینه‌سازی شده این پروتکل، گره‌های بی‌سیم مسیرها را در حافظه نهان [1] خود نگهداری می‌کنند. با آنالیز در مسیرهای موجود در این حافظه می‌توان به برخی از درخواست‌های ارتباط با گره مقصد بدون اجرای فرآیند کشف مسیر پاسخ داد [۲۳].

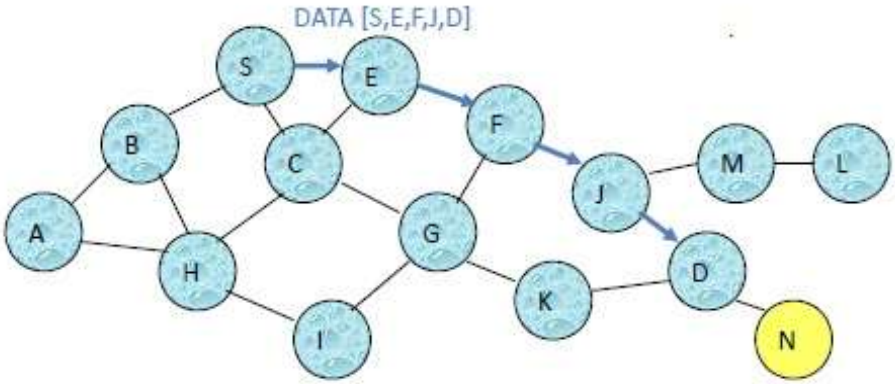


الف

[1] Cash



ب



ب

شکل ۲-۳ فرآیند کلی مسیریابی پروتکل DSR الف) ارسال بسته‌های RREQ ب) دریافت بسته‌های RREP

مسیریابی بردار فاصله مبتنی بر تقاضا (AODV[1]): این الگوریتم یکی دیگر از الگوریتم‌های واکنشی می‌باشد که به دلیل استفاده از ویژگی شماره توالی مقصد به‌نوعی از آلگوریتم DSVD ایده گرفته شده است. در این الگوریتم، فرآیند کشف مسیر تنها زمانی آغاز به کار می‌کند که مسیری بین دو گره وجود نداشته باشد. مسیرها در این الگوریتم تنها در مدت زمانی که مورد استفاده قرار

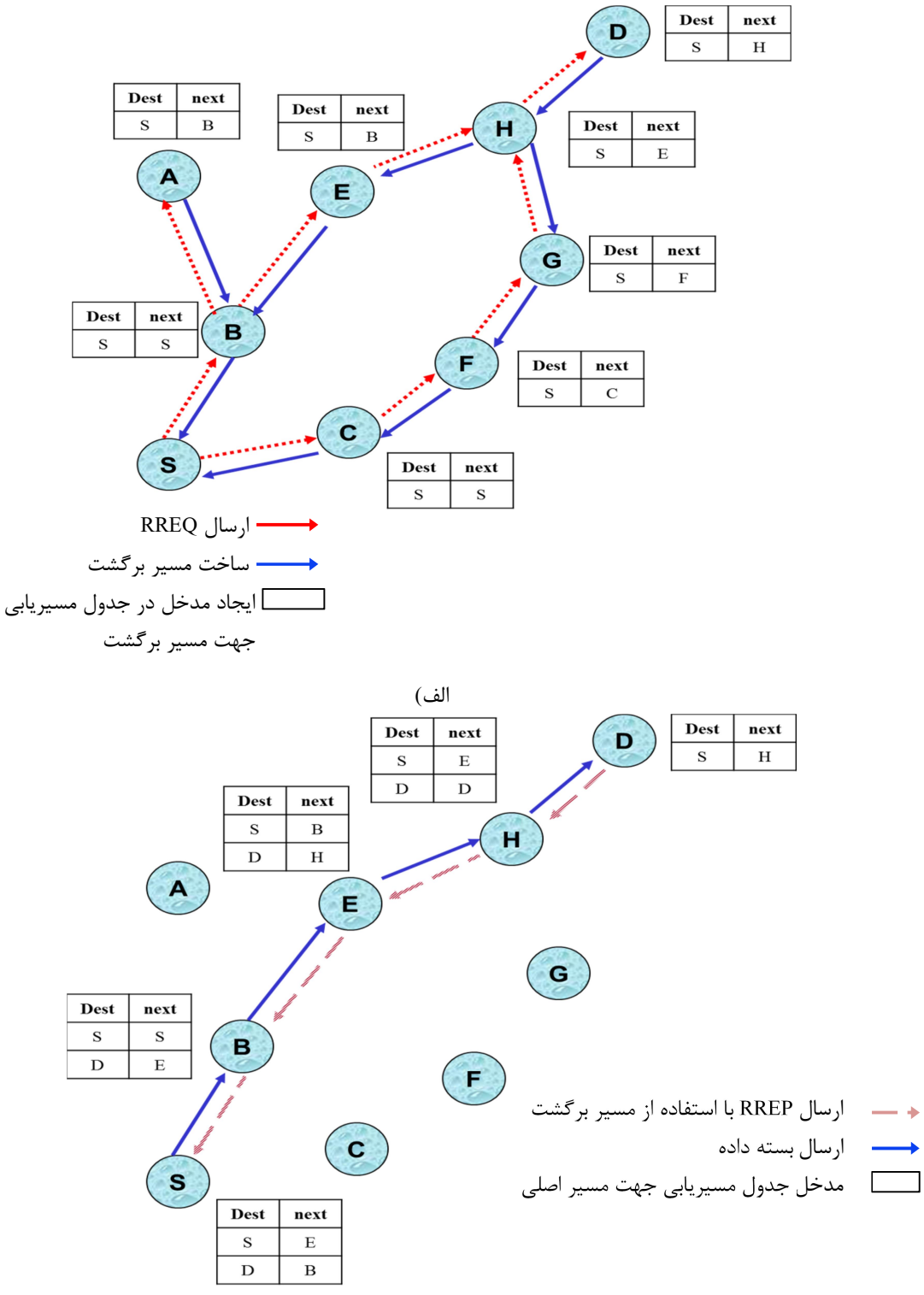
[1] Ad hoc on-demand distance vector

می‌گیرند نگهداری می‌شوند. مسیرها به‌صورت یک ارسال سیل‌آسا کشف می‌شوند. در طی فرآیند مسیریابی، گره‌های شبکه در جستجوی مسیر به سمت مقصد توسط بسته‌های درخواست مسیر RREQ مورد سؤال قرار می‌گیرند .در طی فرآیند کشف مسیر، گره‌های میانی آدرس گره‌ای که بسته REEQ را از آن دریافت کرده‌اند را در جدول مسیریابی خود ذخیره می‌کنند تا در صورت انتخاب این مسیر به‌عنوان مسیر نهایی بسته‌های پاسخ مسیر RREP را به سمت آن ارسال نمایند. بنابراین در ارسال بسته داده، گره مبدأ و گره‌های میانی تنها آدرس گره بعدی خود را نگاه می‌دارند و این‌طور نیست که آدرس کل مسیر را در اختیار داشته باشند. برای جلوگیری از دریافت و پردازش دو یا چندگانه بسته‌های RREQ در یک گره (از طرف چند همسایه) هر درخواست RREQ شامل جفت شناسه کلید RREQ_ID و Node_ID می‌باشد. درصورتی‌که گره‌ای RREQ با این شناسه کلید را از گره دیگری دریافت کرده باشد از پردازش مجدد آن خودداری می‌کند. با انتقال بسته RREQ از یک گره به گره دیگر مقدار ویژگی Hop Count که مبین تعداد گام پیموده شده از مبدأ تا آن گره است یک واحد اضافه خواهد شد. درصورتی‌که در خلال فرآیند کشف مسیر با گره‌ای مواجه شویم که دارای یک مسیر معتبر به مقصد باشد بسته RREP با استفاده از مسیر برگشت ایجاد شده در ارسال RREQ به سمت گره مبدأ به‌صورت تک‌پخشی[1] ارسال خواهد شد. ویژگی Hop Count بسته RREP ارسالی برابر مقدار Hop count آخرین RREQ بعلاوه مقدار ویژگی Hop Count موجود در جدول مسیریابی گره آگاه از مقصد می‌باشد. درصورتی‌که گره مبدأ چند بسته RREP متفاوت از گره‌های دریافت کند، مسیری را انتخاب می‌کند که دارای ویژگی Hop Count کمتری باشد. همچنین به‌منظور جلوگیری از ارسال سیل‌آسای درخواست‌های RREQ در فضای شبکه، هر درخواست RREQ حاوی یک ویژگی به

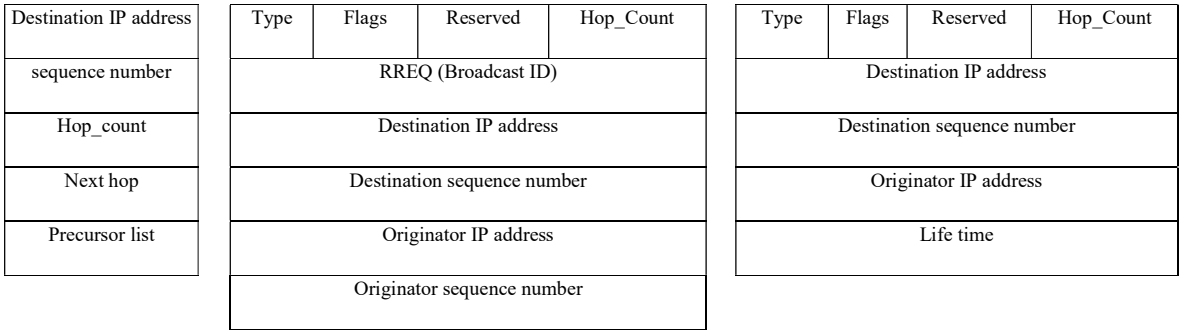
[1] Unicast

نام TTL Number[1] می‌باشد که محدوده گسترش بسته RREQ را مشخص می‌کند. بر اساس یک رابطه زمانی مبتنی بر مقدار TTL گره مبدأ در انتظار بسته RREP تا آن بازه زمانی می‌ماند. در صورت عدم حصول نتیجه و دریافت نکردن RREP، گره مبدأ مجدداً اقدام به ارسال بسته RREQ این بار با TTL Number بیشتر (معمولاً دو برابر مقدار قبلی) خواهد نمود. این فرآیند (اضافه کردن مقدار TTL Number) تا زمانی ادامه پیدا می‌کند که به یک مقدار حدی برای ویژگی TTL[2] برسیم که در آن صورت بسته داده دور انداخته خواهد شد و مشخصات آن از بافر تمام گره‌های درگیر پاک می‌شود. شروع مقدار TTL[3] معمولاً با مقدار ۲ می‌باشد و حد پایان آن ۷ است. در جدول مسیریابی گره‌ها، علاوه بر آدرس گره بعدی تعداد گام‌های مورد نیاز برای رسیدن به مقصد و آخرین شماره توالی استفاده شده ثبت می‌شود. از فیلد شماره توالی جهت کشف تازگی مسیر استفاده می‌شود. در صورت رسیدن بسته RREQ و یا RREP جدید که دارای فیلد شماره توالی بیشتری باشد، گره دریافت‌کننده می‌فهمد که مسیر موجود در آن قدیمی شده است. پروتکل AODV در انتخاب مسیر بهینه به ویژگی تعداد گام[4] نیز توجه می‌کند. بسته فرآیند کلی مسیریابی در پروتکل AODV در دستیابی گره مبدأ S به گره مقصد D در شکل ۲-۴ نشان داده شده است. همچنین مقادیر و پارامترهای مربوط به بسته‌های RREQ و RREP که شامل آدرس مبدأ و مقصد، شماره درخواست در RREQ، شماره مسلسل مبدأ و مقصد، شمارنده گره و طول عمر بسته می‌باشد، به همراه ساختار جدول مسیریابی گره‌ها در شکل ۲-۵ نشان داده شده است [۲۴].

[1] Time To Live (TTL)
[2] TTL threshold
[3] TTL Start
[4] Hop count



شکل ۲-۴ عملکرد کلی پروتکل مسیریابی AODV الف) ارسال بسته‌های RREQ ب) دریافت بسته‌های RREP



بسته RREP　　بسته RREQ　　جدول مسیریابی

شکل ۲-۵ ساختار بسته‌های RREQ و RREP و جدول مسیریابی در پروتکل AODV

با خروج یک گره موجود در مسیر از ناحیه نیز گره‌های همسایه آن که آدرس این گره را به‌عنوان گره بعدی در رسیدن به مقصدی خاص در جدول مسیریابی خود دارند اقدام به ارسال بسته‌های(Rout RERR(Error می‌نمایند. این کار به‌منظور مطلع نمودن گره مبدأ و آغاز مجدد فرآیند مسیریابی توسط آن انجام می‌شود. همچنین، در صورتی که گره‌ای که متوجه شکست در اتصال شد چنانچه به گره مقصد نزدیک باشد، می‌تواند فرآیند مسیریابی مجدد را خود انجام دهد. شناسایی گره‌های همسایه نیز از طریق ارسال بسته‌های Hello Message انجام خواهد شد. همچنین مسیرها در این پروتکل دارای یک عمر زمانی[1] هستند. درصورتی‌که در مدت تعیین‌شده، به آن مسیر رجوع نشود مسیر موردنظر از مدخل جدول مسیریابی گره حذف خواهد شد.

۲-۱-۲-۴- پروتکل‌های ترکیبی

این مورد با ترکیب دو روش قبلی سعی در کاهش معایب هریک از انواع پروتکل‌های مسیریابی کرده و از ویژگی‌های خوب هر دو مورد بهره می‌برد. معروف‌ترین پروتکل از این نوع می‌توان به پروتکل مبتنی بر منطقه ZRP [2] اشاره کرد. این پروتکل از ویژگی‌های نوع پیش کنشی برای مسیریابی گره‌های

[1] Life time
[2] Zone routing protocol

نزدیک به هم و از ویژگی‌های نوع واکنشی برای مسیریابی گره‌های دورتر استفاده می‌کند. این پروتکل به‌نوعی مبتنی بر خوشه‌بندی[1] نیز می‌باشد [۵].

۲-۱-۲-۵-حملات لایه شبکه

در یک تقسیم‌بندی می‌توان حملات موجود در شبکه‌های موردی سیار و به‌نوعی کلیه شبکه‌های کامپیوتری را به دو دسته غیرفعال[2] و فعال[3] تقسیم کرد [۱۱]. که حمله نوع غیرفعال، حمله‌ای انفعالی به‌حساب می‌آید و گره‌ای که این حمله را انجام می‌دهد شاید هیچ اقدام خرابکارانه‌ای برای برهم زدن منطق مسیریابی و یا ترافیک شبکه انجام ندهد و تنها با رصد کردن بسته‌های اطلاعاتی ردوبدل شده در شبکه به‌نوعی به استراق سمع می‌پردازد ولی یک حمله نوع فعال به‌وضوح اقدام به خرابکاری در منطق مسیریابی شبکه و یا ترافیک آن می‌نماید. با توجه به این تعریف واضح است که حملات نوع غیرفعال نسبت به حملات نوع فعال به‌سختی قابل‌تشخیص هستند هرچند که این حملات نیز درصدی از تغییر در منطق مسیریابی شبکه و یا ترافیک آن را، خواهد داشت. در زیر برای برخی از این حملات که احتمالاً در این تحقیق استفاده خواهند شد توضیح کوتاهی ارائه می‌شود.

حمله ارسال سیل‌آسا[4]: با توجه به اینکه پیغام‌های RREQ و RREP در شبکه‌ها اعتبار سنجی نمی‌شوند لذا گره‌های حمله‌کننده می‌توانند با استفاده از این پیغام‌ها اقدام به ارسال سیل‌آسای آن به شبکه کنند که این امر سبب بروز مشکلات ذیل می‌شود [۲۵]:

- از کار انداختن شبکه با استفاده از دست‌کاری کردن منطق مسیریابی آن
- اشغال بی‌مورد پهنای باند شبکه

---

[1] Clustring
[2] Passive
[3] Active
[4] Flood storm attack

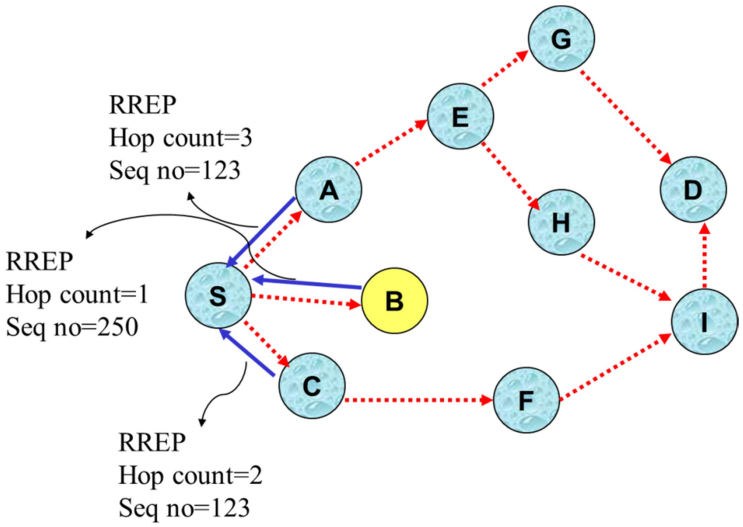
حمله انهدام و تغییر بسته‌ها[1]: برای گره‌های میانی این امکان وجود دارد که اقدام به تغییر و دست‌کاری محتویات بسته نمایند. با توجه به اینکه استفاده از الگوریتم‌های کنترل مجموع[2] را نمی‌توان روی این شبکه‌ها اعمال نمود، لذا گره‌های میانی می‌توانند علاوه بر آن اقدام به تغییر و دست‌کاری اطلاعات سرآیند بسته‌ها نمایند. در این شبکه‌ها برخلاف شبکه‌های سیمی که مکانیزم مشخصی برای گره‌های مسیریاب وجود داشت هر گره‌ای می‌تواند عمل مسیریابی را انجام دهد و با این امکان اقدام به معدوم نمودن بسته‌های داده و مسیریابی نماید. این حمله برحسب فرکانس و یا نوع انتخاب بسته‌های معدوم شونده توسط حمله‌کننده به انواع زیر تقسیم می‌شود [۲۶].

- انهدام انتخابی
- انهدام با فرکانس ثابت
- انهدام با فرکانس متناوب
- انهدام با فرکانس تصادفی

حمله سیاه‌چاله[3]: این حمله از طریق یکی از گره‌های موجود در شبکه اعمال می‌شود. به این نحو که این گره با ارسالRREP مساعد به هر RREQ دریافتی بدون توجه کردن به جدول مسیریابی خود و بدون توجه به اینکه آیا این گره مسیری به گره مقصد دارد یا خیر باعث کوتاه شدن زمان ارسال بسته‌های RREP نسبت به گره‌ای دیگر می‌شود. با زودتر رسیدن بسته RREP ارسالی از این گره، گره فرستنده این گره را به‌عنوان مسیر مناسب و کوتاه برای ارسال بسته‌ها تشخیص داده و بسته‌های خود را از مسیر این گره ارسال می‌کند. در این صورت یک سیاه‌چاله ایجاد شده است و گره متخاصم به‌جای ارسال بسته‌ها به مقصد اقدام به دریافت اطلاعات آن‌ها و دور انداختن آن‌ها می‌کند. به‌عنوان‌مثال در شکل زیر. گره S قصد ایجاد مسیری به گره D را دارد. در این حال گره S پیغام RREQ را به گره‌های

[1] Packet Modifications and Dropping
[2] Checksum
[3] Black hole

همسایه جهت جستجوی گره D پخش همگانی[1] می‌کند. گره متخاصم B بدون در نظر گرفتن جدول مسیریابی خود با یک شماره توالی بالا و تعداد گام[2] برابر یک به RREQ ورودی جواب RREP می‌دهد. البته این RREP از طرف گره D و یا گره دیگری که از آدرس آن اطلاع دارد هم ارسال می‌شود، اما محتویات بسته RREP آن‌ها احتمالاً دارای تعداد گام بیشتر، شماره توالی کمتر و در زمان دیرتری نسبت به RREP ارسالی از B فرستاده خواهد شد. با ورود این بسته‌ها به گره S طبیعی است که این گره مسیر بهتر که از طرف گره متخاصم B ارسال شده است را انتخاب می‌کند. بعد از این، گره B اقدام به استراق سمع و انهدام بسته‌های دریافتی می‌کند. فرآیند کلی موجود در حمله سیاه‌چاله در شکل ۲-۶ نشان داده شده است. در نوع دیگری از این حمله که توسط دو گره متخاصم صورت می‌گیرد (در شکل d نشان داده شده است) گره متخاصم اول B1 ممکن است بجای آنکه خود بسته‌های دریافتی را منهدم کند، آن‌ها را به B2 بفرستد. این کار به‌جهت پایین آوردن احتمال شناسایی آن انجام می‌گیرد [۲۷].



شکل ۲-۶- نحوه عملکرد حمله Black-Hole

[1] Broad cast
[2] Hop Count

حمله کرم‌چاله[1]: این حمله توسط دو گره صورت می‌گیرد. گره اول ابتدا با ارسال یک سیگنال رادیویی مجزا به گره دوم یک تونل ارتباطی ایجاد می‌کند. کلیه بسته‌های ارتباطی که به گره اول می‌رسد به‌صورت مستقیم به گره دوم نیز فرستاده می‌شود. لذا، با توجه به ارسال مستقیم و مجزای بسته‌ها از طریق این اتصال فاصله میان این دو گره یک گام فرض می‌شود. این خدعه سبب ارسال بسته‌های RREQ از طرف همسایه‌های گره مبدأ اول به سمت همسایه‌های گره دوم می‌شود و بالعکس می‌شود. گره‌های متخاصم در این حالت می‌توانند آسیب بیشتری را به شبکه تحمیل کنند[۲۸].

۲-۱-۳-لایه پیوند داده

همان‌طور که در بخش ۲-۳ مطرح شد لایه پیوند داده در شبکه‌های بی‌سیم وظیفه ایجاد یک بستر پایدار، کارآمد با بهره‌وری مناسب جهت انتقال داده در کانال مشترک بین گره‌ها را دارد. با توجه به اینکه کانال مشترک بین گره‌ها در یک فضای همسایگی معنی پیدا می‌کند بنابراین لازم است تا اطلاعاتی راجع به محدوده‌های رادیویی اطراف یک گره بی‌سیم در شبکه‌های موردی سیار و نواحی ایجادشده توسط آن‌ها داشته باشیم. هر گره بی‌سیم در این نوع از شبکه‌ها دارای دو شعاع رادیویی فیزیکی استاندارد با نام شعاع رادیویی انتقال[۲] و شعاع رادیویی گوش دادن[۳] و یک شعاع مجازی به نام شعاع رادیویی تداخل[۴] می‌باشد. در ذیل به توضیح هریک از شعاع‌های رادیویی توضیح داده شده و نواحی ایجادشده در اطراف آن می‌پردازیم [۱۳ و ۱۴].

---

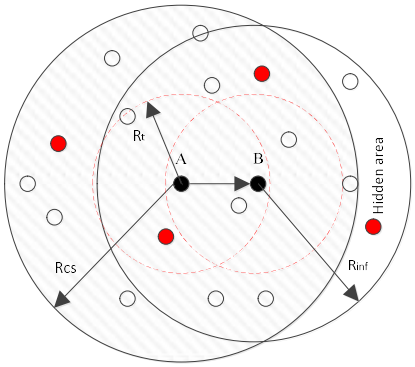
[1] Wormhole attack
[2] Transmission range
[3] Carrier sensing range
[4] Interference range

- **شعاع رادیویی انتقال**: بیانگر شعاع رادیویی است که یک گره می‌تواند داده‌ای را در صورت عدم تداخل سیگنال، با موفقیت دریافت کند. به محدوده ایجادشده به ازای این شعاع رادیویی، محدوده انتقال و یا محدوده دریافت[1] گفته می‌شود. همچنین مجموعه گره‌های موجود در این محدوده، گره‌های همسایه[2] می‌نامند. شعاع رادیویی انتقال معمولاً با استفاده از توان انتقال[3] که از مشخصه‌های انتقال رادیویی یک محصول می‌باشد تعیین می‌گردد.
- **شعاع رادیویی حساسیت گوش دادن**[4]: شعاع رادیویی است که به ازای آن هر انتقال صورت گرفته در محدوده آن سبب فعال شدن حسگر انتقال در گره بی‌سیم خواهد شد و گره موردنظر ما توانایی گوش دادن به این انتقال را خواهد داشت. شعاع این محدوده توسط مشخصه حساسیت آنتن[5] مشخص می‌شود. درصورتی‌که گره‌ای، انتقالی را در این محدوده تشخیص دهد، از انتقال داده خود صرف‌نظر خواهد کرد.
- **شعاع رادیویی تداخل**[6]: مسئله اصلی در وجود این شعاع رادیویی آن است که وجود انتقال در تمام محدوده حساسیت گوش دادن سبب بروز تداخل در دریافت سیگنال داده توسط آن نمی‌شود. درصورتی‌که گره A شروع به دریافت داده نماید و در این حین، انتقال داده دیگری در محدوده شعاع رادیویی تداخل گره A صورت پذیرد سبب بروز تداخل در دریافت داده توسط گره A خواهد شد. محدوده رادیویی تداخل در اطراف گره گیرنده ایجاد می‌شود. این شعاع رادیویی برخلاف دو شعاع رادیویی دیگر از مشخصه‌های استاندارد یک گره بی‌سیم نیست و اندازه آن بستگی به فاصله بین گره گیرنده و فرستنده دارد. درصورتی‌که دو گره

---

[1] Capture area
[2] Neighbor nodes
[3] Transmission power
[4] Carrier sensing range
[5] Antenna sensitivity
[6] Interference range

گیرنده و فرستنده خیلی به هم نزدیک باشند ممکن است که این ناحیه عملاً وجود نداشته باشد و با بیشتر شدن فاصله میان گیرنده و فرستنده مساحت این ناحیه بیشتر خواهد شد.



شکل ۲-۷ فضای همسایگی بین چند گره در ارسال داده از طرف گره A به B به همراه محدوده‌های رادیویی مورد استفاده

با در نظر گرفتن این سه شعاع رادیویی به‌طور طبیعی سه ناحیه نیز ایجاد خواهد شد که در توضیح هر شعاع به ذکر آن پرداختیم. در شکل ۲-۷ هریک از این سه ناحیه مشخص شده است. سه شعاع بررسی‌شده به ترتیب با R_t، R_{cs} و R_{inf} مشخص شده‌اند. همان‌طور که در شکل مشخص است، از برهم‌کنش این سه ناحیه ممکن است دو ناحیه دیگر نیز ایجاد شود که این دو ناحیه مخفی[1] و ناحیه تزاحم[2] نام دارند. همان‌طور که از شکل ۲-۷ برمی‌آید در انتقال داده از گره A به سمت گره B، قسمتی از ناحیه تداخل گره B که توسط ناحیه گوش دادن گره فرستنده A پوشش داده می‌شود را ناحیه تزاحم و مابقی آن که پوشش داده نمی‌شود را ناحیه مخفی گویند. کانال ارتباطی بی‌سیم میان گره‌ها در آن واحد تنها می‌تواند به یک گره اختصاص داشته باشد. درصورتی‌که گره‌ای در ناحیه مخفی اقدام به ارسال داده به هر گره دلخواه دیگری کند، این ارسال از دید گره فرستنده A مخفی بوده و دریافت داده را در گره گیرنده (B) با برخورد مواجه می‌کند. این مشکل برای گره‌های موجود در ناحیه

[1] Hidden area
[2] Interfering area

تزاحم پیش نخواهد آمد. این مورد به‌این‌علت است که گره‌های موجود در این ناحیه در محدوده گوش دادن گره A هستند و هرگونه انتقال داده از طرف آن‌ها از دید گره A مخفی نخواهد ماند. برای رفع این مشکل مکانیزم های زیادی جهت کار در لایه انتقال داده ارائه شده است. همان‌طور که از مطالب گفته شده برمی‌آید ارسال داده در یک فضا همسایگی از گره‌های بی‌سیم نیازمند رعایت سازوکارهای متعددی است که امکان یک ارتباط عادلانه و کارآمد را بین گره‌های موجود در یک فضای همسایگی فراهم کند. به همین منظور پروتکل‌های متعددی جهت کار در این لایه ارائه شده است که از بین آن پروتکل IEEE 802.11 DCF به‌عنوان بروزترین پروتکل پایه موردبررسی قرار می‌گیرد.

۲-۱-۳-۱- پروتکل IEEE 802.11 DCF

بر اساس مرسوم‌ترین پروتکل ارائه شده که تحت عنوان استاندارد IEEE 802.11 DCF ارائه شده، از دو تکنیک جلوگیری از ازدحام (Collision Avoidance-CA) و گوش دادن به کانال جهت دسترسی چندگانه (Carrier Sensing Multiple Access-CSMA) استفاده می‌کند. در قسمت CA از مکانیزم هایی مانند دست‌تکانی چهار مرحله‌ای RTS/CTS[۱] و دومرحله‌ای BA[۲] و مکانیزم به تعویق انداختن[۳] ارسال بسته استفاده می‌شود. همچنین بر اساس تکنیک CSMA به‌منظور کاهش احتمال برخورد در ارسال داده گره کانال را قبل از ارسال بسته‌های کنترلی به‌صورت فیزیکی به ازای بازه‌های زمانی مشخص به‌منظور اطمینان از خالی بودن آن پایش می‌کند. این کار از طریق اندازه‌گیری انرژی موجود در کانال انجام می‌شود. همچنین به‌منظور کاهش هزینه پایش کانال، از یک مکانیزم پایش مجازی با بکارگیری بردار به نام NAV[۴] استفاده می‌شود.

---

[1] Request to send/Clear to send
[2] Basic Access
[3] Backoff mechanism
[4] Network allocation vector

عملکرد این الگوریتم بر اساس مکانیزم RTS/CTS به این صورت است که گره فرستنده جهت ارسال بسته داده بعد از اطمینان از صفر بودن مقدار NAV، ابتدا لازم است کانال را به مدت یک بازه زمانی DIFS[1] پایش کند. جهت ادامه کار، لازم است تا در این بازه کانال ارسال داده آزاد باشد. این کار از طریق مکانیزم گوش دادن[2] با رصد انرژی موجود در کانال صورت می‌گیرد. سپس به‌منظور کاهش احتمال تصادم در ارسال بسته، گره ارسال خود را به‌اندازه k برش زمانی که k به‌صورت یکنواخت از بازه [0 CW] انتخاب می‌شود، به تعویق می‌اندازد. بنابراین کل مدت زمانی که گره ارسال خود را به تعویق می‌اندازد برابر با $k.T_S$ می‌باشد. اندازه هر برش زمانی T_S[3] از مشخصه‌های سخت‌افزاری لایه پیوند داده می‌باشد. CW[4] نشان‌دهنده حداکثر پنجره انتظار تعویق که از رابطه ۲-۱ محاسبه خواهد شد.

$$CW = (CW_{min} + 1).2^{RC} - 1 \qquad (۱-۲)$$

که در آن CW_{min} نشان‌دهنده حداقل پنجره انتظار تعویق جهت به تعویق انداختن ارسال داده می‌باشد. RC[5] نیز نشان‌دهنده تعداد تلاش مجاز جهت ارسال داده است که با هر بار شکست در ارسال آن به تعداد یک واحد به مقدار آن افزوده می‌شود. در صورت اتفاق افتادن یک تلاش موفق مقدار RC به صفر تنظیم خواهد شد. مقدار CW نیز در واقع با تنظیم مقدار RC تعیین خواهد شد. این مقدار می‌تواند به ssrc (station short-frame retry counter) برای بسته‌های با حجم کم و یا slrc (station long-frame retry counter) برای بسته‌های با حجم زیاد محدود گردد. با گذر زمان از تعداد برش زمانی‌هایی که یک گره باید ارسال داده را به تعویق بیاندازد، کاسته می‌شود و در یک فضای رقابتی گره‌ای که زودتر مقدار پنجره انتظار تعویق آن به صفر رسید اجازه ارسال پیدا می‌کند. در ابتدای هر

[1] DCF Interframe Space
[2] Carrier sensing
[3] Time slice
[4] Contention Window
[5] Retry Counter

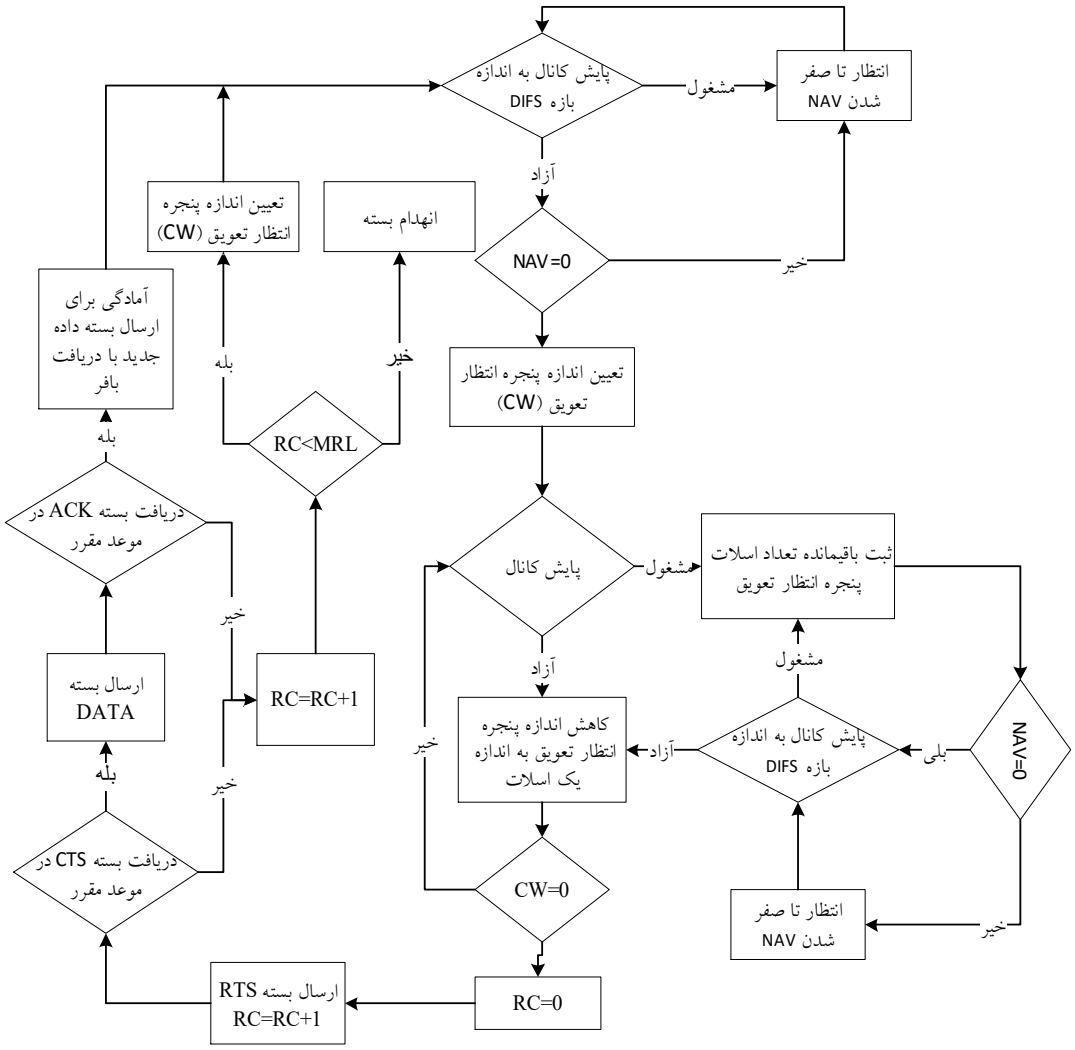
برش زمانی، گره کانال را پایش می‌کند. درصورتی‌که کانال خالی بود (انرژی موجود در کانال از یک حد خاصی کمتر بود) به فرآیند کاهش تعداد برش زمانی ادامه می‌دهد. در غیر این صورت عدد تعداد برش زمانی باقی‌مانده برای گره ثابت شده تا در رقابت بعدی دارای اولویت بالاتری باشد. در صورت موفقیت گره در پایش کانال به‌اندازه برش زمانی DIFS و گذراندن پنجره انتظار تعویق، گره آمادگی خود را برای ارسال داده با فرستادن بسته RTS با پخش همگانی آن اعلام می‌کند. گره گیرنده، به‌مجرد دریافت آن، بعد از اینکه کانال را به‌اندازه بازه زمانی SIFS خالی پایش کرد، بسته CTS را بصورت پخش همگانی ارسال می‌کند. کلیه گره‌های موجود در محدوده گره‌های فرستنده و گیرنده با شنیدن بسته‌های RTS و CTS مقدار مشخصه NAV را به عددی تنظیم می‌کند که جهت یک انتقال کامل داده و دریافت تأییدیه آن (بسته ACK) کافی باشد. در صورت موفقیت‌آمیز بودن فرآیند RTS/CTS گره فرستنده اقدام به ارسال بسته داده می‌کند و بعد از دریافت کامل آن توسط گره گیرنده، بسته کنترلی ACK از طرف آن ارسال خواهد شد. عملکرد کلی مکانیزم RTS/CTS در شکل ۲-۸ نشان داده شده است.

مکانیزم BA نیز کم‌وبیش به همین صورت خواهد بود با این تفاوت که بسته فرستنده بدون نیاز به ارسال بسته RTS و دریافت بسته CTS از طرف گیرنده، بعد از اطمینان از صفر بودن مقدار NAV، آزاد بودن کانال به‌اندازه DIFS و موفقیت در رقابت تعویق ارسال، بسته داده را ارسال می‌کند و فرستنده نیز با دریافت موفقیت‌آمیز آن، بسته ACK را ارسال خواهد کرد.

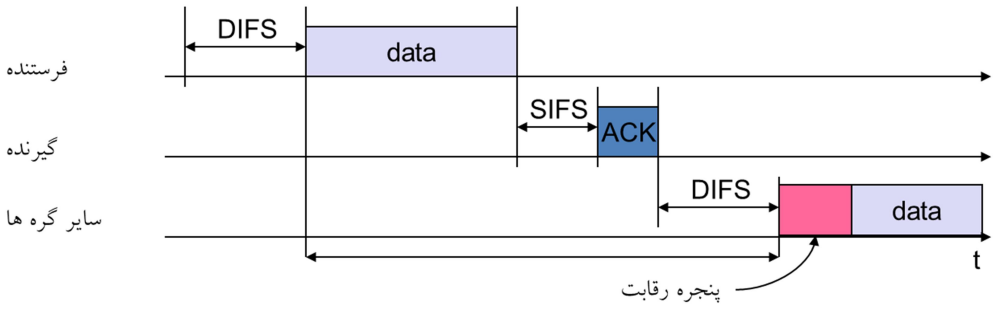
همان‌طور که توضیح داده شد، مکانیزم گوش دادن به کانال به‌صورت مجازی و بدون پایش و اندازه گیری انرژی موجود در کانال با استفاده از بردار NAV نیز انجام می‌شود. NAV درواقع یک تایمر است که با تنظیم آن توسط هر گره، با گذشت زمان از مقدار آن کم می‌شود و استفاده از آن به‌طور چشم‌گیری باعث کاهش احتمال تصادم در ارسال داده با صرف انرژی بسیار کم خواهد شد. هر گره با

شنیدن یکی از بسته‌های کنترلی RTS و CTS و یا بسته داده مقدار تایمر NAV را به نحوی تنظیم می‌کند که تا دریافت بسته ACK با وارسی آن نیاز به پایش کانال نداشته باشد.

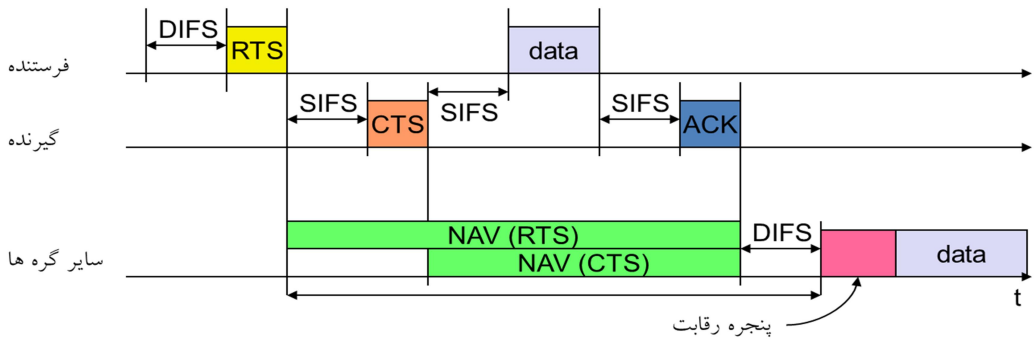
همان‌طور که از شکل ۲-۹ (الف) برمی‌آید در مکانیزم RTS/CTS هر گره با شنیدن بسته RTS مقدار NAV را به $3.\mathrm{SIFS} + \mathrm{T_{CTS}} + \mathrm{T_{Data}} + \mathrm{T_{ACK}}$ و با شنیدن بسته CTS آن را به $2.SIFS + T_{Data} + T_{ACK}$ تنظیم می‌کند و در مکانیزم BA نیز همانطور که در شکل ۲-۹ (ب) نشان داده شده با ارسال داده توسط گره فرستنده، گره‌های دیگر مقدار تایمر NAV را به $SIFS + T_{Data} + T_{ACK}$ تنظیم خواهند کرد [۳۰،۲۹].



شکل ۲-۸ فلوچارت عملکرد پروتکل IEEE 802.11 DCF به ازای مکانیزم دست تکانی چهار مرحله‌ای RTS/CTS



الف)



ب)

شکل ۲-۹ عملکرد گره‌ها در تنظیم مقدار تایمر NAV استفاده از الف) مکانیزم BA ب) مکانیزم RTS/CTS

۲-۱-۳-۲-حملات لایه پیوند داده

اساس کار پروتکل IEEE 802.11 DCF بر این اصل استوار است که تمام گره‌های موجود در یک همسایگی از قوانین مشروع این پروتکل پیروی می‌کنند. در این حال ممکن است بعضی گره‌های متخاصم با دست‌کاری در قوانین این پروتکل، موجب ایجاد اولویت بالاتر نسبت به گره‌های مشروع شوند. اولویت موردنظر این گره‌ها معمولاً جهت دستیابی به کانال جهت ارسال داده می‌باشد که سبب بالا رفتن میزان بهره‌وری شبکه[1] برای این گره‌ها خواهد شد. بالا رفتن بهره‌وری برای این گره‌ها متخاصم بالطبع سبب کاهش بهره‌وری شبکه برای گره‌های نرمال خواهد شد. گره‌های متخاصم می‌توانند در سرتاسر شبکه و در هریک از همسایگی‌های ایجادشده وجود داشته باشند و با تغییر پارامترهای پروتکل IEEE 802.11 DCF به مقصود موردنظرشان برسند. پارامترهای موردنظر این گره‌ها معمولاً شامل پنجره انتظار تعویق[2]، تایمر NAV، بازه انتظار DIFS و سرعت ارسال داده[3] می‌باشد. در ذیل به جزئیات عملکرد هریک از این حملات می‌پردازیم [۳۱].

[1] Network throughput
[2] Contention window
[3] Data transmission speed

حمله دست‌کاری طول پنجره انتظار تعویق: در این نوع از حمله گره متخاصم سعی در کوچک کردن طول پنجره انتظار تعویق که به ازای آن گره ارسال داده خود را به تعویق می‌اندازد، دارد. طول پنجره انتظار تعویق بر اساس رابطه ۲-۱ توسط الگوریتم موجود در پروتکل IEEE 802.11 DCF مشخص می‌شود. در نوعی از این حمله، گره متخاصم تعداد برش‌های زمانی پنجره انتظار تعویق را از محدوده $[0, \gamma CW]$ انتخاب می‌کند که در آن $(0 \leq \gamma < 1)$. در نوع دیگری از این حمله گره متخاصم با هر بار عدم موفقیت در ارسال داده بر اساس آنچه در رابطه ۲-۱ مشخص شده طول پنجره انتظار تعویق را دو برابر نمی‌کند که این امر منجر به کوتاه‌تر شدن طول پنجره انتظار تعویق برای این گره نسبت به گره‌های دیگری که موفق به ارسال موفقیت‌آمیز نشده‌اند، می‌شود. استفاده از هریک از این دو روش سبب بالا رفتن اولویت گره متخاصم در دستیابی به کانال نسبت به گره‌های مشروع خواهد شد.

حمله دست‌کاری طول تایمر NAV: در این نوع از حمله گره متخاصم با شنیدن بسته‌های کنترلی RTS و یا CTS مقدار تایمر NAV خود را به نحوی تنظیم می‌کند که احتمال بروز تصادم در مرحله بعدی الگوریتم برای گره مشروعی که اکنون کانال را در اختیار دارد، وجود داشته باشد.

حمله دست‌کاری بازه انتظار DIFS: در این نوع از حمله گره متخاصم بازه انتظار DIFS را قبل از عملیات تعویق انجام نمی‌دهد و یا آنکه در زمان کوتاه‌تری از زمان معمول این کار را انجام می‌دهد. این کار به میزان قابل‌توجهی سبب بالا رفتن شانس گره متخاصم در تصاحب کانال خواهد شد.

حمله تغییر سرعت ارسال داده: در این نوع از حمله گره متخاصم که کانال را در اختیار دارد، داده خود را با سرعت پایین‌تر و یا بالاتر از استاندارد تعیین‌شده توسط پروتکل IEEE 802.11 DCF ارسال می‌کند. این کار سبب ایجاد تداخل در ارسال داده توسط گره‌های مشروع دیگر که منتظر آزاد شدن کانال توسط این گره متخاصم هستند و تایمر NAV را خود را به‌درستی تنظیم کرده‌اند خواهد شد. با

توجه به اینکه با احتمال زیادی کانال مورد استفاده ظرفیت ارسال داده با سرعت بالاتر را ندارد گره‌های متخاصم معمولاً در این نوع از حمله، داده خود را با سرعت پایین‌تر ارسال می‌کنند که این امر سبب تداخل در ارسال داده توسط گره‌های مشروع خواهد شد.

۲-۲- شبکه‌های پتری

نظریه شبکه‌های پتری برای اولین بار در سال ۱۹۶۲ توسط کارل آدام پتری [1] بعنوان یک رساله مقطع دکتری در دانشگاه دارم آلمان ارائه شد. این نظریه در دهه ۱۹۷۰ در دانشگاه MIT بسط داده شد. در حال حاظر فعالیت‌های تحقیقاتی خوبی در رابطه با کاربرد شبکه‌های پتری در مدل‌سازی سیستم‌های توزیع شده، پروتکل‌های ارتباطی، سیستم‌های صنعتی و محاسبات الگوریتمی صورت گرفته است. با ظهور ایده‌های جدید در نظریه شبکه‌های پتری و گسترش قابلیت‌های آن تحت عنوان کلاس‌های جدید، امکان مدل‌سازی سیستم‌های بیشتری فراهم شده است. امکانات زیادی به مدل اولیه شبکه پتری اضافه شده است تا قدرت مدل‌سازی آن را افزایش یابد و بتوان آن را در زمینه‌های مختلف به کار برد.

استفاده از شبکه‌های پتری در مواردی می‌باشد که هدف مطالعه سیستمی به‌منظور کسب اطلاعات شاخص درباره ساختار و رفتار سیستم مدل شده و استخراج معیارهای ارزیابی از آن می‌باشد. ویژگی‌ها و مفاهیم شبکه پتری به‌گونه‌ای است که آن‌را روشی ساده و قوی برای توصیف و تحلیل جریان اطلاعات و کنترل سیستم‌هایی که با فعالیت‌های آسنکرون [2] و یا سنکرون سروکار دارند معرفی کرده است. شبکه‌های پتری علاوه بر اینکه دارای ساختار و رفتار صوری هستند، قابلیت نمایش گرافیکی نیز دارند که به همین سبب مدل‌سازی توسط آنها آسان شده است. یکی از دلایل موفقیت شبکه‌های پتری سادگی آنهاست که البته این سادگی گاه مدل کردن سیستم‌های

[1] Carl Adam Petri
[2] Asynchronous

پیچیده را دشوار می‌سازد. همچنین چارچوب ریاضی شبکه پتری سبب می‌شود تا توانایی تحلیل, تایید صحت و ارزیابی مدل‌ها را نیز داشته باشد.

در ساده‌ترین شکل، یک شبکه پتری (PN) گراف جهت‌داری با دو مجموعه مجزا شامل مکان[۱] و گذار[۲] می‌باشد. کمان[۳]های جهت‌دار در این گراف مکان‌ها را به گذارها (کمان‌های ورودی نامیده می‌شوند) و گذارها را به مکان‌ها (کمان‌های خروجی نامیده می‌شوند) اتصال می‌دهند. مکان‌ها ممکن است حاوی یک عدد صحیح با هویتی بنام نشانه[۴] باشند. حالت یا وضعیت سیستم به حضور یا عدم حضور نشانه در مکان‌های مختلف در یک شبکه پتری وابسته است. وضعیت حضور نشانه در مکان‌ها بعضی از گذارها را قادر به فعال شدن[۵] می‌سازد. فعال شدن گذارها منجر به برداشت نشانه‌ها از یک یا چند مکان و ورود نشانه‌ها به یک یا چند مکان دیگر در شبکه خواهد شد. بعد از فعال شدن یک گذار، نشانه‌ها از مکان-های متصل به گذار بوسیله کمان ورودی برداشت شده و به مکان‌های متصل به گذار بوسیله کمان‌های خروجی وارد می شوند. علامت‌گذاری[۶] یک PN در واقع توزیع نشانه‌ها در مکان‌های آن است. علامت-گذاری نمایشی بوسیله یک بردار $M=(m(P_1),m(P_2), \ldots ,m(P_n))$ می باشد که در آن $m(P_i)$ تعداد نشانه‌ها در مکان i و n تعداد مکان‌ها در شبکه را نشان می‌دهد. [۳۳,۳۲].

۲-۲-۱-تعریف رسمی از شبکه پتری پایه و خصوصیات آن

تعاریف رسمی متفاوتی برای یک شبکه پتری وجود دارد. در یک تعریف رسمی، یک شبکه پتری پایه ترکیبی از چهار جزء می‌باشد: مجموعه‌ای از مکانها (P)، مجموعه‌ای از گذارها (T)، یک تابع ورودی (I) و یک تابع خروجی(O)

---

[1] Place
[2] Transition
[3] Arc
[4] Token
[5] Fire
[6] Marking

توابع I/O پل ارتباط گذارها (T) و مکانها (P) بوده و آن‌ها را به‌هم مرتبط می‌کند. تابع وردی I «یک نگاشت از گذار t_j به مجموعه مکانهای$I(t_j)$ است» که به عنوان مکانهای ورودی گذار شناخته می باشد. تابع خروجی O «یک نگاشت از گذارt_j به یک نمونه از مکانهای$O(t_j)$ است» که به مکانهای خروجی شناخته می‌شوند. ساختار یک شبکه پتری پایه بوسیله مکان‌ها، گذارها، توابع ورودی و خروجی تعریف می‌شوند مکان P_i یک مکان ورودی از گذار t_j است اگر $P_i \in I(t_j)$ باشد و یک مکان خروجی است که اگر $P_i \in O(t_j)$ باشد. شکل ۲-۱۰ ساختار یک شبکه پتری مفروض را نشان می دهد[۳۴].

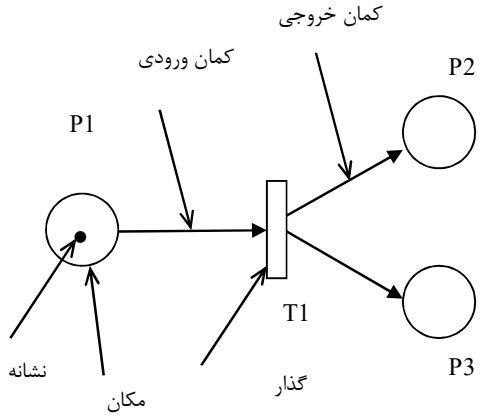
$P = \{P_1, P_2, \dots \dots . P_n\}, n \geq 0$

$t = \{t_1, t_2, \dots \dots . P_m\}, m \geq 0$

$P \cap T = \emptyset$

$I: P^{\infty} \rightarrow T$

$O: T \rightarrow P^{\infty}$



شکل ۲-۱۰: مثالی از ساختار یک شبکه پتری

۲-۲-۲-مشخصه‌های ساختاری شبکه‌های پتری

یکی از خصیصه های بارز شبکه‌های پتری فراهم آوردن ابزارهایی تحلیلی جهت مطالعه و تحلیل مشخصه های اصلی یک سیستم است. بعد از مدل سازی سیستم توسط یک شبکه پتری، لازم است

تا مدل ساخته شده جهت برآوردن ویژگی های ساختاری و رفتاری آن مورد مطالعه قرار گیرد. این ویژگی‌ها شامل چند دسته مشخص می باشند که از قرار زیر است.

قابلیت دسترسی[1]: این خصیصه بعنوان یک رفتار پایه ای جهت مطالعه امکان پویایی یک سیستم بکار می رود. اجرای یک گذار فعال، موقعیت سیستم را براساس قوانین فعال سازی تغییر خواهد داد و علامت‌گذاری جدیدی را ایجاد خواهد کرد. یک علامت‌گذاری قابل دسترسی از علامت‌گذاری دیگر است اگر یک توالی پیوسته از گذارها وجود داشته باشد که نتیجه آن انتقال از علامت گذاری اولیه به علامت‌گذاری جدید باشد. مجموعه علامت‌گذاری های[2] قابل دسترس یک شبکه پتری با n مکان را فضای حالت شبکه پتری گویند. مجموعه (گرافی) از علامت‌گذاری های قابل دسترس از علامت گذاری اولیه (M_0) را با $RS(M_0)$ نشان می‌دهند.

کراندار بودن[3]: یک شبکه پتری با علامت گذاری اولیه M_0، کراندار با درجه K[4] خوانده می شود که اگر عدد مثبت K وجود داشته باشد که به ازای تمام $p_i \in P$ رابطه $M'(p_i) \leq k$ برقرار باشد. M' در این‌جا یک علامت گذاری از پتری می‌باشد. در تعریف بالا در صورتی که $k=1$ باشد شبکه پتری را مطمئن[5] گویند. بنابراین تعریف مطمئن بودن یک شبکه پتری با 1-Bounded بودن آن یکسان است.

یک مکان P_i کراندار (کرانه K) است اگر و تنها اگر

$$\forall M \in RS(M_0), \quad \exists k : m_i \leq k \qquad (۲-۲)$$

یک پتری‌نت کراندار(کرانه K) است اگر و تنها اگر

$$\exists k : (\forall P_i \in P : \text{کرانه} k \text{است}) \qquad (۳-۳)$$

---

[1] Reachibility
[2] Marking
[3] Boundedness
[4] k-bounded
[5] Safe

زنده بودن[1]: این مفهوم اغلب در سیستم های تخصیص منابع که امکان بروز بن بست[2]در آن وجود دارد اتفاق می افتد. مشابه با مفهوم بن بست در سیستم عامل، این مفهوم در شبکه پتری به معنای دسته ای از گذارها می باشند که امکان فعالیت آنها وجود ندارد. گذارهایی که هیچ گاه در موقعیت بن بست قرار نمی گیرند، زنده نامیده می شوند. در یک شبکه پتری زنده، برای هر توالی از گذارهای فعال، امکان اجرای بدون بن بست تضمین می شود.. یک گذار t_r زنده است اگر و تنها اگر

$$\forall M \in RS(M_0)\,, \quad \exists M' : (M \xrightarrow{s} M' \wedge tr \in E(M')) \qquad (۴-۲)$$

یک پتری‌نت زنده است اگر و تنها اگر

$$\forall t_r \in T : t_r \text{زنده باشد}$$

یک علامت‌گذاری M زنده است اگر و تنها اگر

$$\forall t_r \in T\,, \quad \exists M' : (M \xrightarrow{s} M' \wedge t_r \in E(M')) \qquad (۵-۲)$$

همچنین یک پتری‌نت زنده است اگر

$$\forall M \in RS(M_0) : M \text{زنده باشد}$$

وضعیت خانه [3]: یک شبکه پتری را در وضعیت خانه گویند در صورتی که علامتگذاری با نام M' وجود داشته باشد که از هر علامتگذاری M قابل دسترس باشد. در بسیاری از کاربردها خصوصاً مدل سازی سیستم های کارخانه ای ممکن است نیاز باشد تا به یک موقعیت مشخص از سیستم فرضاً با نام M' برگردیم. خاصیت وضعیت خانه این خصوصیت را برای سیستم مدل شده فراهم می‌کند. در

[1] Liveness
[2] Deadlock
[3] Home State

صورتی که در تعریف بالا $M' = M^0$ باشد در آن صورت شبکه پتری را **برگشت پذیر**[1] گویند.یک علامت‌گذاری M_h یک وضعیت خانه نامیده شده است اگر و تنها اگر

$$\forall M' \in RS(M0), \quad M_h \in RS(M') \qquad (۶-۲)$$

مجموعه‌ای از وضعیت‌های خانه پتری‌نت فضای حالت خانه[2] نامیده می شود .شبکه پتریی که دارای خواص کراندار، زنده و برگشت پذیر باشد را **خوش رفتار**[3] گویند.

استفاده از روابط جبر خطی

استفاده از جبر خطی برای تحلیل مدل های شبکه پتری براساس ماتریس اندیس[4]شبکه پتری صورت می گیرد که نمایشی ماتریسی از یک شبکه پتری به حساب می آید. این شیوه نمایش دهنده ارتباط میان ساختار شبکه پتری و رفتار آن است. این شیوه نمایش از پتری به همراه معادلات و نامعادلات جبر خطی را می توان جهت نشان دادن رفتار و خصوصیات آن استفاده کرد. معادلات جبر خطی یک شبکه پتری ماتریس با استفاده از ماتریس اندیس بیان شود. ماتریس اندیس C از یک پتری‌نت با m مکان و n گذار بصورت یک ماتریس m*n است. همچنین ستون‌های ماتریس C نشان‌دهنده گذارها و سطرها ی ماتریس نیز نشان‌دهنده مکان‌ها است و مقادیر آن به شکل زیر مشخص می‌شود:

$$C(p,t) = O(t,p) - I(t,p) \qquad (۷-۲)$$

مقدار C(p,t) در ماتریس C نمایش‌دهنده یک مقدار مثبت یا منفی است که تغییر تعداد نشانه در مکان P را بعد از اجرای گذار t نشان می‌دهد..

---

[1] Reversibility
[2] home space
[3] well behaved
[3]Incidence matrix

برای هر علامت‌گذاری M ، فعال شدن یک گذار t و ایجاد علامت گذاری جدید M' با استفاده از ماتریس اندیس از طریق رابطه ذیل انجام می‌شود [۳۴].

$$M' = M + C(.,t)^T \qquad (۸-۲)$$

گاهی در یک شبکه پتری توالی اجرای گذارها و یا تعداد نشانه در مکان ها معانی خاصی را در بر دارد. این موارد در نهایت منجر به تعریف روابط ثابت برای یک شبکه پتری خواهد شد که با ناوردایی مبتنی بر مکان[۱] و ناوردایی مبتنی بر گذار[۲] بیان می‌شوند.

ناوردایی مبتنی بر مکان: این ویژگی ناظر بر مجموعه مکان‌هایی است که تعداد نشانه در آن‌ها بدون توجه به ترتیب اجرای گذارها و یا اینکه در چه علامت‌گذاری باشم مقدار ثابتی است.

$$\sum_{p=1}^{p} m_p = \sum_{p=1}^{p} m_{0p} \quad , \quad \forall M \in RS(M_0) \qquad (۹-۲)$$

یک پتری‌نت محافظه‌کار(یکسان) است اگر و تنها اگر

$$\exists Y = (y1, y2, \ldots, yp) > 0 \qquad (۱۰-۲)$$

که در آن

$$\sum_{p=1}^{p} y_p m_p = \sum_{p=1}^{p} y_p m_{0p} \quad , \quad \forall M \in RS(M_0) \qquad (۱۱-۲)$$

از این وابستگی نتیجه می‌شود که :

$$M \xrightarrow{t_r} M' \quad \equiv \quad M' = M + [C_r]^T \Rightarrow Y[M']^T = Y[M]^T + Y[C_r] \qquad (۱۲-۲)$$

---

[1] P- Invarient
[2] T- Invarient

مقدار صحیح Y از معادله $YC = 0$ ، ناوردای مبتنی بر مکان نامیده شده است .یک شبکه پوشیده بوسیله یک ناوردای مبتنی بر مکان کراندار خواهد بود. صرف نظر از ویژگی‌های ساختاری، ناوردایی مبتنی بر مکان ، برای سیستم های مختلف مدل شده توسط یک شبکه پتری این خصیصه می‌تواند معانی متفاوتی داشته باشد.

ناوردایی مبتنی بر گذار: این ویژگی ناظر بر گذارهایی است که ترتیب اجرای آن‌ها، یک شبکه پتری را در همان وضعیت اولیه (قبل از اجرای گذارها) بر می گرداند. با فرض اینکه $V = (V1, V2, \ldots, VT)^T$ تعداد گذار برداری وابسته به مراحل فعالیتS باشد

(۱۳-۲)

$$M \xrightarrow{t_r} M' \quad \equiv \quad M' = M + [C_r]^T$$

$$M \xrightarrow{s} M'' \quad \equiv \quad M'' = M + [CV]^T$$

مقدار صحیح X از معادله $CX = 0$ استخراج می‌شود مجموعه ناوردایی مبتنی بر گذار یک شبکه پتری می‌باشد. یک شبکه که بوسیله یک ناوردای مبتنی بر گذار پوشیده شده ممکن است وضعیت خانه باشد. همانند ناوردایی مبتنی بر مکان این ویژگی نیز برای سیستم های مختلف مدل شده توسط یک شبکه پتری می‌تواند معانی متفاوتی داشته باشد.

۲-۲-۳-شبکه‌های پتری تصادفی[1] و تصادفی تعمیم یافته[2]

شبکه‌های پتری تصادفی به عنوان یک مدل توسعه یافته از شبکه‌های پتری پایه و بمنظور افزودن امکانات مدل‌سازی به آن معرفی شده است. در این نوع از شبکه‌های پتری، گذارها بعد از امکان بالقوه فعال شدن دارای تأخیر در اجرا می‌باشند. تأخیر فعال شدن گذارها در این حالت، معمولاً بوسیله

[1] Stochastic Petri Net (SPN)
[2] Generalized Stochastic Petri Net (GSPN)

متغیرهای تصادفی با تابع شدت احتمال نمایی منفی, مشخص می‌شوند. در این شبکه‌ها به هر گذار T_i، یک تأخیرفعال‌شدن بطور تصادفی نسبت داده می‌شود که احتمال آن یک تابع نمایی منفی با نرخ λ_i است. ویژگی بدون حافظه تابع شدت احتمال نمایی منفی، امکان توصیف مفید و متفاوت‌تری از مدل‌های شبکه‌های پتری تصادفی را فراهم می کند.. در زمان فعال‌سازی گذار، زمان سنج با سرعتی ثابت کاهش می‌یابد. اگر فعال شدن یک گذار مخالف، آن را غیر فعال کند زمان سنج متوقف شده و در حین فعال‌سازی مجدد گذار فرآیند کاهش احتمالاً با سرعتی متفاوت از سر گرفته می‌شود. هنگامی که زمان سنج به صفر نزدیک می‌شود، گذار فعال می‌گردد. با شبیه‌سازی ساختار یک سیستم توسط شبکه پتری تصادفی می‌توان اطلاعات مفیدی را با تحلیل آن استخراج کرد. از این اطلاعات می‌توان بمنظور ارزشیابی، بهبود و یا تغییرات در سیستم استفاده کرد.

در تعریف رسمی مرسوم، یک شبکه پتری تصادفی یک شش‌تایی مرتب به شکل $\{M_0 ، O ، I ، T ، P$ $\lambda\}$ معرفی می شود. در این تعریف $M_0 ،O ،I ،T ،P$ همانند شبکه پتری اولیه معرفی شده در بخش ۲-۲-۱ می‌باشد. $\lambda= \{ \lambda_1 , \lambda_2 , \ldots , \lambda_n \}$ نیز معرف مجموعه نرخ فعال‌شدن گذارها می‌باشد.

شبکه‌های پتری تصادفی با همه توفیقات خود در بعضی موارد برای مدل‌سازی سیستم‌های پیچیده دچار مشکل بوده‌اند. از جمله، در یک سیستم واقعی مواردی وجود دارد که فعالیت ها و یا گذارها دارای زمان نیستند. بعنوان مثال در مواردی که بخواهیم از بین دو یا چند رویداد ممکن بدون توجه به زمان آن‌ها یک حالت را انتخاب کنیم. همچنین در مورد دیگر، در صورتی که نیاز به اعطای اولویت به یک یا چند گذار یا فعالیت در یک شبکه پتری نسبت به گذارهای دیگر باشد توسط شبکه پتری تصادفی ممکن نبود.

در نوع کامل‌تری از شبکه پتری تصادفی به‌نام شبکه پتری تصادفی تعمیم‌یافته[1] گذارها به دو گروه گذارهای آنی[2] و زمان‌دار[3]، تقسیم می‌شوند. گذارهای آنی با ▮ و گذارهای زمان‌دار با▯ نشان داده می‌شوند. گذارهای آنی در صورت فراهم شدن شرایط بلافاصله فعال می شوند، در حالیکه گذارهای زمان‌دار بعد از یک مقدار که با نرخ احتمال نمایی منفی مشخص می شوند، قادر به فعال شدن هستند.

همچنین این نوع از شبکه پتری دارای یک تابع اولویت می‌باشد که سطوح اولویت را به گذارها نسبت می‌دهد و در حالت پیش فرض گذارهای زمانی دارای اولویت صفر (کمترین اولویت) هستند. ویژگی دیگر شبکه پتری های تصادفی تعمیم یافته استفاده از کمان بازدارنده میباشد. یک کمان بازدارنده یک کمان از یک مکان به یک گذار است که فعال شدن گذار را منوط به نبود نشانه (یا وجود نشانه کمتر از یک حد خاص) در مکان می‌کند.

بطور رسمی شبکه پتری تصادفی تعمیم یافته یک هشت تایی بصورت $\{ P, T, \rho, I, O, H, M_0, W \}$ که در آن (P, T, I, O, M_0) مانند شبکه‌های پتری است, البته مجموعه (T) به دو زیرمجموعه T_1 و T_2 تقسیم شده ، که به‌ترتیب نشان‌دهنده مجموعه گذارهای آنی و گذارهای زمان‌دار می‌باشند. و H مجموعه کمانهای بازدارنده بصورت $H \subset P \times T$ و تقدم‌های گذار به گذارها، ρ نیز نشان‌دهنده مجموعه تقدم گذارها می باشد. $W = (w_1, w_2, ..., w_n)$ ، یک مجموعه برای محاسبه احتمالات فعال شدن گذارهای آنی استفاده می‌شود. در یک شبکه درصورتی‌که هر دو گذارهای آنی وزمانی فعال شده باشند، گذارهای آنی بر گذارهای زمان‌دار اولویت دارند.

---

[1] Generalized Stochastic Petri Net (GSPN)
[2] Immediate Transition
[3] Timed Transition

اجمان مارسان[1][۷۲] نشان‌داده است که یک شبکه پتری تصادفی تعمیم یافته در قدرت با زنجیره مارکوف پیوسته معادل است. هر زنجیره مارکوف پیوسته می‌تواند به یک شبکه پتری تصادفی تعمیم یافته معادل تبدیل شود و هرمدل شبکه پتری تصادفی تعمیم یافته نیز می‌تواند به یک زنجیره مارکوف پیوسته معادل تبدیل شود. با توجه به وجود تکنیک‌های مشابه جهت حل زنجیره مارکوف پیوسته برای حالت‌های ثابت، گذرا و انباشته و معیارهای حساسیت یک زنجیره مارکوف پیوسته می-تواند درحل معیارهای مشابه یک شبکه پتری تصادفی تعمیم یافته استفاده شود.

مشخصات یک زنجیره مارکوف پیوسته مرتبط با یک شبکه پتری تصادفی تعمیم یافته با استفاده از اعمال قوانین ساده زیر بدست می‌آید [۳۲].

- فضای حالت زنجیره مارکوف پیوسته با مجموعه علامت‌گذاری های قابل دسترس $RS(M_0)$ از پتری‌نت تصادفی تعمیم یافته مطابقت دارد.
- نرخ گذار از حالت s_i (متناظر با علامت‌گذاری M_i) به حالت s_j برابر است با مجموع نرخ‌های فعال‌شدن (برای گذارهای زمان‌دار) یا وزن‌های (برای گذارهای آنی) گذارهایی که در M_i فعال شده است و فعال شدن آنها منجر به تولید علامتگذاری M_j شده است.

بر اساس قوانین ساده ذکر شده در بالا، می‌توان اقدام به ایجاد ماتریس نرخ گذار زنجیره مارکوف پیوسته متناظر با یک شبکه پتری تصادفی تعمیم یافته کرد.

فرض می کنیم U ماتریس مربوط به تابع انتقال وضعیت‌ها در زنجیره مارکوف پیوسته متناظر، Q ماتریس متناظر با نرخ انتقال تبدیل وضعیت، $_k$، نرخ فعال شدن و یا احتمال مرتبط با گذار T_k (گذاری که فعال شدنش شبکه را از حالت علامت‌گذاری M_i به علامت‌گذاری M_j منتقل می کند) و

[1]Ajmone Marsan

$E_j(M_i)$ نیز مجموعه این گذارها باشد. در این‌صورت اجزاء ماتریس متناظر با احتمال و نرخ تبدیل وضعیت با استفاده از روابط زیر بدست می‌آید:

$$U_{ij} = \frac{\sum_{T_{ik} \in E_j(M_i)} W_k}{q_i} \qquad (۱۴-۲)$$

$$q_{ij} = \begin{cases} \sum T_k \epsilon E_j(M_i) w_k & i \neq j \\ q_i & i = j \end{cases} \qquad (۱۵-۲)$$

$$q_i = \sum_{T_k \in E(M_i)} w_k$$

همچنین مدت زمان سپری شده در یک وضعیت علامتت‌گذاری (M_i) از مدل زنجیره مارکوف پیوسته ایجاد شده از مدل شبکه پتری تعمیم یافته از رابطه زیر بدست می‌آید.

$$SJ_{i=1}/_{q_i} \qquad (۱۶-۲)$$

مجموعه وضعیت‌های موجود در گراف دسترسی ایجاد شده از یک شبکه پتری تصادفی به دو نوع : **قابل اعتنا**[1] و **غیر قابل اعتنا**[2] طبقه‌بندی می‌شوند. وضعیت M_i قابل اعتنا گفته می‌شود اگر مجموعه گذارهای خروجی که این وضعیت را به وضعیت دیگری منتقل می کنند همگی زمان‌دار باشند. در این صورت زمان سپری شده در این وضعیت بزرگتر از صفر خواهد بود. مجموعه وضعیت هایی وجود دارند که زمان سپری شده در آن برابر صفر است. این وضعیت ها تنها با فعال شدن یک گذار آنی به وضعیت دیگر منتقل می شوند و از این‌رو غیر قابل اعتنا نامیده می شوند. در هر علامتگذاری انتخاب اینکه کدام گذار فعال شده براساس تقدمات و وزنها می باشد. مجموعه گذارهای دارای بیشترین سطح اولویت در ابتدا اجرا می‌شوند و اگر این مجموعه شامل بیش از یک گذار باشد انتخاب بعدی، بوسیله احتمال و براساس وزنهای گذار طبق عبارت زیر خواهد بود:

---

[1] Tangible
[2] Vanishing

$$P\{t_k\} = \frac{W_k}{q_i} \qquad (۱۷-۲)$$

در صورتی که RS، TRS وVRS به‌ترتیب نشان‌دهنده مجموعه قابل دسترسی، مجموعه قابل دسترسی وضعیت‌های قابل اعتنا و مجموعه قابل دسترسی وضعیت‌های غیر قابل اعتنا باشد رابطه زیر برقرار است :

$$RS = TRS \cup VRS \text{ and } VRS \cap TRS = \emptyset \qquad (۱۸-۲)$$

۲-۲-۴-ارزیابی یک شبکه پتری تصادفی تعمیم یافته

استخراج معیارهای ارزیابی از یک شبکه پتری تصادفی با تناظر آن به مدل زنجیره مارکوف پیوسته معادل صورت می‌پذیرد که شیوه این تبدیل در بخش قبل توضیح داده شده است. اکثر معیارهای ارزیابی قابل استخراج از احتمال حالت پایدار[1] وضعیت‌های مدل زنجیره مارکوف استفاده می کنند. مقدار احتمال پایدار مرتبط با هر وضعیت با حل سیستم معادلات خطی زیر بدست می‌آید. در صورتی که گراف قابلیت دسترسی مدل شبکه پتری تصادفی تعمیم یافته پس اصلاح آن و حذف وضعیت‌های غیر قابل اعتنا شامل n وضعیت باشد در آن رابطه ذیل n+1 معادله n-مجهولی را تولید می‌کند [۳۲].

$$\eta Q = 0 \qquad \sum_i \eta_i = 1 \qquad (۱۹-۲)$$

η_i، نشان‌دهنده احتمال حالت پایدار علامتگذاری M_i می‌باشد و Q نیز ماتریس نرخ مرتبط با انتقال وضعیت‌ها در زنجیره مارکوف پیوسته است که نحوه استخراج آن در بخش قبل توضیح داده شد. استخراج هریک از معیارهای ارزیابی از رابطه کلی ۲-۲۰ بدست می‌آید که در آن r_i ناظر بر تابع پاداش متناظر با هر معیار ارزیابی و η_i نیز احتمال حالت پایدار مرتبط با وضعیتی از زنجیره مارکوف است که به ازای آن شرط r_i ارضا شده است.

[1] Steady state probability

$$E[R] = \sum_{i \epsilon \Omega_T} r_i \eta_i \qquad (۲۰-۲)$$

احتمال مرتبط با برقراری یک شرایط خاص در یک شبکه پتری تصادفی: با فرض اینکه شرایط Y(M) در یکسری از علامتگذاری‌های پتری‌نت درست است، تابع پاداشی زیر را می‌توان تعریف نمود:

$$r(M) = \begin{cases} 1 & , Y(M) = \text{true} \\ 0 & , \text{otherwise} \end{cases} \qquad (۲۱-۲)$$

احتمال دلخواه $P=\{Y\}$ با استفاده از معادله محاسبه شده است. که به صورت زیر بیان می شود:

$A=\{M_i \epsilon RS(M_0): Y(M_i) = \text{true}\}$.

$$P\{Y\} = \sum_{M_i \epsilon A} \eta_i \qquad (۲۲-۲)$$

مقدار مورد انتظار تعداد نشانه در یک مکان مشخص : در این مورد، تابع پاداش r(M)برای مکان j ام مقدار j ام خانه در هر علامت‌گذاری است

$$r(M) = n \quad \text{if } M(p_j) = n \qquad (۲۳-۲)$$

این معادل شناسایی زیرمجموعه A(j,n) از $RS(M_0)$ است که در مکان p_j تعداد n نشانه وجود دارد. مقدار مورد انتظار نشانه‌ها در p_j از رابطه ۲-۲۴ بدست می‌آید. بدیهی است $n \leq k$ در صورتی‌که مدل شبکه پتری کراندار با درجه k باشد.

$$E[M(P_j)] = \sum_{n>0}[n \ P\{A(j,n)\}] \qquad (۲۴-۲)$$

متوسط تعداد اجرای یک گذار در واحد زمان: برای بدست آوردن فرکانس فعالیت گذار T_j (توان گذردهی گذار T_j) برای محاسبه خواسته شده، تابع پاداش در اینجا مقدار w_j در تمام هرعلامت‌گذاری هایی است که به ازای آن T_j فعال شده است:

$$r(M) = \begin{cases} W_j & , T_j \epsilon E(M) \\ 0 & , otherwise \end{cases} \qquad (۲۵-۲)$$

مقدار متوسط فعالیت T_j در واحد زمان از رابطه زیر بدست می‌آید :

$$f_i = \sum_{M_i \epsilon A_j} W_j \ \eta_i \qquad (۲۶-۲)$$

بدست آوردن این معیارها نشان می‌دهد که شبکه‌های پتری علاوه بر امکان توصیف رفتار سیستم‌ها و ارزیابی خواص کیفی آن‌ها بعنوان یک ابزار برای محاسبه شاخص‌های کارآیی که وسیله برای ارزیابی بهره‌وری سیستم‌ها است نیز استفاده می‌گردد.

۲-۲-۵-شبکه‌های تصادفی مبتنی بر پاداش[1]

SRN [۳۵] بطور قابل ملاحظه‌ای قدرت مدل سازی شبکه‌های پتری تصادفی تعمیم یافته را افزایش داده است. از جمله قابلیت‌های اضافه شده امکاناتی مانند استفاده از توابع نگهبان، وزن کمان‌های مبتنی بر یک تابع شرطی و یا مبتنی بر مقدار توکن در یک مکان , اولویت گذاری عمومی گذارها و تعیین تابع پاداش در سطح شبکه می‌باشد. تابع نگهبان یک تابع بولی منتسب به یک گذار است. هر زمان که همه شرایط فعال شدن یک گذار فراهم شده باشد در صورت ارضاء شرط موجود در تابع حفاظت مربوطه اجرا خواهد شد.

SRN قابلیت مدل سازی یکسان مانند مدل زنجیره مارکوف مبتنی بر پاداش را ارائه می‌دهد. رابطه تابع پاداش برای هر سیستمی متفاوت می‌باشد و معمولاً ترکیبی از معیارهای ارزیابی توضیح داده شده در بخش قبل می باشد که برای ارزیابی یک سیستم مدل شده توسط SRN می‌توان از آن استفاده کرد. علاوه بر معیارهایی که در بخش قبل توضیح داده شده چند معیار دیگر نیز می‌توان با تبدیل یک SRN به یک مدل مارکوف مبتنی بر پاداش استخراج کرد. این معیارها عبارتند از نرخ مورد انتظار

[1] Stochastic Reward Net (SRN)

پاداش در حالت پایدار و یا در یک زمان مشخص، مقدار مورد انتظار تجمعی پاداش تا زمان جذب یا در یک زمان مشخص , توزیع تجمعی پاداش تا زمان جذب و یا در یک زمان مشخص.

مقدار مورد انتظار پاداش در حالت پایدار براساس فرمول زیر بدست می‌آید. به ازای این رابطه مقدار نرخ پاداش در تمام علامت گذاریهای قابل اعتنا محاسبه خواهد شد

$$E[R] = \sum_{i\epsilon\Omega_T} r_i\eta_i \qquad (۲۷-۲)$$

مقدار مورد انتظار پاداش در زمان t با محاسبه احتمال گذرای[1] از بودن در هر علامت‌گذاری $i \epsilon \Omega_T$, Ω_T محاسبه خواهد شد. مقدار مورد انتظار نرخ پاداش در زمان t بوسیله فرمول زیر بدست می‌آید:

$$E[R(t)] = \sum_{i\epsilon\Omega_T} r_i\eta_i\,(t) \qquad (۲۸-۲)$$

توزیع نرخ پاداش در زمان t , $P\{R(t)\leq x\}$ بوسیله فرمول زیر بدست می‌آید:

$$P\{R(t) \leq x\} = \sum_{r_i\leq x\,,i\in\Omega_T} \eta_i\,(t) \qquad (۲۹-۲)$$

توزیع تجمعی نرخ پاداش تجمعی در بازه $[0,t]$ که با $Y(t)$ نشان داده می شود براسا رابطه ذیل بدست می‌آید.

$$E[Y(t)] = E[\int_0^t R(u)du] = \int_0^t E[R(u)]du = \sum_{i\epsilon\Omega_T} r_i \int_0^t \eta_i\,(u)du \qquad (۳۰-۲)$$

۲-۲-۶-شبکه‌های پتری فازی

شبکه پتری معمولی با منطق کلاسیک[2] سازگاری دارد ، در حال‌که در عمل با سیستم‌های پیچیده‌ای سرو کار داریم که در توصیف آنها درجه‌ای از نااطمینانی وجود دارد . بنابراین برای توصیف چنین سیستم‌هایی با استفاده از شبکه پتری لازم است تا این نااطمینانی‌های برحسب عبارات مبهم و

[1] Transient probability
[2] Classical

غیردقیق در مدل پتری نمایش داده شود. این امر مستلزم معرفی مفهوم فازی در مدل پتری می‌باشد. از این رو در سال ۱۹۸۸ لونی و همکاران[1] [۷۳] سیستم فازی طراحی کردند که کم وبیش با نظریه شبکه های پتری سازگاری داشت. همه این شیوه‌های مختلف که شبکه‌پتری و مجموعه‌های فازی را با هم ترکیب می‌کنند شبکه پتری‌فازی نامیده میشود. اختلاف این شبکه‌های‌پتری‌فازی در عناصری است که فازی شده اندو در یک شبکه پتری فازی هریک از مفاهیم گذار ،مکان‌ها ، نشانه‌ها وکمانها می‌توانند فازی شوند [۳۶].

۲-۲-۶-۱-انواع عناصر فازی در شبکه پتری فازی

یک **نشانه فازی**[2] یک تعمیم از نشانه در شبکه پتری استاندارد میباشد . درشبکه پتری استاندارد مقدار نشانه متعلق به مجموعه {۱و۰}است . در حالیکه یک نشانه فازی میتواند ارزشی مابین فاصله[۱و۰] را اخذ کند. در نوع فازی‌تر می‌توان به‌یک نشانه یک عبارت حرفی نظیر کم، متوسط ، زیاد ، نسبت داد که به هریک از آنها یک تابع عضویت نسبت داده شده است . این تابع عضویت میزان عضویت از یک مکان با درستی فرضیه را معین می‌کند.

یک **مکان‌فازی**[3] یک گزاره یا ویژگی مربوط به آن مکان را دارد . یک نشانه درآن مکان توسط آن ویژگی وعددی که نشاندهنده میزان عضویت آن نشانه به گزاره مربوط به‌آن مکان است مشخص می شود.

یک **گذار فازی**[4] متناظر با یکسری قواعد فازی به شکل if - Then میباشد و توسط مقادیر درستی متناظر با الگوریتم های استنتاج فازی تحقق می‌یابد .در شبکه پتری معمولی در زمان فعال شدن یک گذار نشانه از مکان مبدأ برداشته شده و به مکان مقصد اضافه می‌شود ولی در منطق

---

[1] Looney
[2] Fuzzy Token
[3] Fuzzy Place
[4] Fuzzy Transaction

فازی به این علت که درستی یک قضیـــه حتـــی بعـد از فعال شدن یک قاعده حفظ می‌شود نشانه درمکان متناظر برداشته نمی‌شود . البته در بعضی از کارهـا کـه قواعـد تولید فازی را نشان میدهد نشانه برداشته میشود . در اغلب کارها یک عامل اطمینـان بـه هـر گذار مربوط میشود , زیرا یک گذار در شبکه پتری متناظر با یک قـــاعده در سیســـتمهایی بـا قواعـد تولیـد می‌باشد که در واقع احتمال فعال شدن را نشان میدهد . در بعضی از شبکه‌های‌پتری‌فازی یـــک زمـان فازی به هر گذار نسبت داده شده و بوسیله مقایسه‌کردن این زمان با زمان جاری مشخص میشود که

۱- آیا گذار متناظر فعال شده است .

۲- احتمالا گذار فعال شده است .

۳- گذار متناظر مطمئنـاً فعال شده است .

یک **کمان فازی**[1] مقدار مورد نیاز یک نشـــانه را مشـخص می‌کنـد . اگر نشـانه بـه طـور دقیـق بـا نیازمندی همخوانی نداشته باشد پس یک مقدار تقریبی به صورت فاصله مابین نشانه و مقدار مورد نیاز محاسبه میشود و اگر فاصله بزرگتر از یک و مقدار بیشینه از پیش تعریف شده باشد گذار می‌تواند اجرا شود .

بطور رسمی یک شبکه پتری فازی بصورت یک ۸تایی تعریف شده است :

$FPN = (P, T, D, I, O, cf,\alpha,\beta)$

که در آن $P =\{ p_1,p_2, \ldots, p_n\}$ نشان‌دهنده یک مجوعه محدود غیرتهی از مکان‌ها است.

$T = \{t_1,t_2,\ldots,t_m\}$ نشان‌دهنده یک مجموعه محدود غیرتهی از گذارها می باشد.

[1]Fuzzy Arc

$P \cap T \cap D = \emptyset$ یک مجموعه محدود غیرتهی از گزاره‌ها یا فرضیه ها می‌باشد. $D = \{ d_1, d_2, \ldots, d_n \}$ و $| D | = | P |$.

$I = \{T \rightarrow P\}$ یک نگاشت ورودی (نشاندهنده تابع ورودی از گذارها به مکان‌ها)، و $O = \{ P \rightarrow T$ {یک نگاشت خروجی (نشاندهنده تابع خروجی از مکان‌ها به گذارها) است.

$cf: T \rightarrow [0, 1]$ یک نگاشت انجمنی (تابع ارتباطی که مقدار یک گذار را به ارزش واقعی (بین صفر تا یک) منتسب می‌کند.

$\alpha: p \rightarrow [0 , 1]$ یک تابع ارتباطی است که مقدار یک مکان را به ارزش واقعی (بین صفر تا یک) منتسب می‌کند.

$\beta: P \rightarrow D$ نیز یک تابع ارتباطی از مکان‌ها به گزاره‌ها است.

در ساده ترین شکل استفاده از یک شبکه پتری فازی مقدار نشانه درمکان $Pi \in P$ توسط[۱و۰ $\in \alpha$ (Pi)] نشان داده میشود. با فعال شدن هر گذار مرتبط کننده مکان‌های *Pi* و *Pj* دارای درجه اطمینان $cf(T_{i,j})$ مقدار α (Pi) از رابطه ۲-۳۱ بدست خواهد آمد.

$$\alpha(P_j) = cf(T_{i,j}) \times \alpha(P_i) \qquad (۳۱-۲)$$

فصل ۳–پژوهش‌های پیشین

در این بخش توضیح اجمالی روی کارهای پیشین انجام شده در حوزه موضوع تحقیق ارائه خواهد شد. با توجه به مدل ارائه شده در فصل ۴، در مرور کارهای انجام شده روی تحقیقات ارائه شده در زمینه ارزیابی کارایی شبکه‌های موردی سیار در دو لایه پیوند داده و شبکه تأکید شده است. همچنین به جهت نبود و یا کمبود تحقیقات انجام شده در موضوع رساله، به تحقیقات انجام شده با موضوعات عمومی‌تر نیز پرداخته شده است. به همین منظور تحقیقاتی مانند استفاده از مدل‌های مارکوف و یا تکنیک‌های جبر خطی و یا تحقیقاتی که تنها به بررسی عملکرد شبکه‌های سیار در زمینه چالش‌هایی مانند مسئله گره مخفی می‌پردازند نیز بررسی شده‌اند.

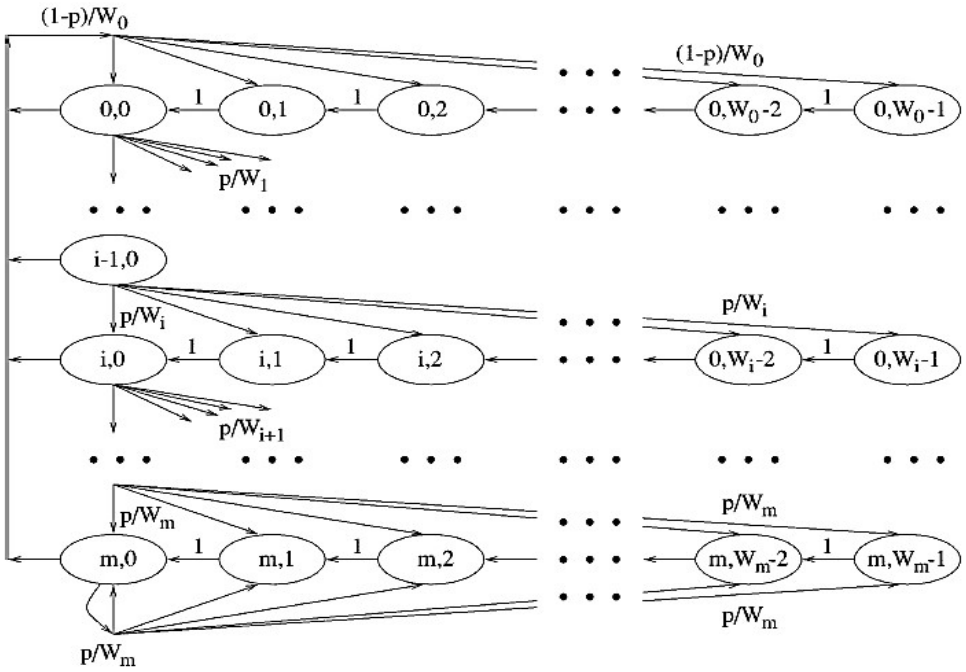
۳-۱- ارائه مدل تحلیلی جهت ارزیابی لایه پیوند داده:

لایه پیوند داده به جهت نزدیک‌تر بودن به سطح لایه فیزیکی و کاهش سطح انتزاع آن از قابلیت مدل‌سازی بیشتری نسبت به لایه شبکه برخوردار است و طبعاً کارهای انجام شده بیشتری در این زمینه وجود دارد. همان‌طور که در بخش ۲-۱-۳ توضیح داده شد الگوریتم‌های استفاده شده در این بخش اغلب دارای رویکردی ترتیبی و نظام‌مند می‌باشند که این مسئله کار مدل‌سازی را در این لایه راحت‌تر می‌کند.

بیانچی[1] در مرجع [۳۷] برای اولین بار اقدام به ارائه یک مدل تحلیلی جامع به‌منظور مطالعه عملکرد پروتکل IEEE 802.11 DCF نمود. در این تحقیق که بعدها مورد توجه بسیاری از پژوهشگران در این زمینه قرار گرفت یک مدل زنجیره مارکوف دو-بعدی برای بررسی عملکرد مکانیزم انتظار تعویق ارائه شده که در شکل ۳-۱ نشان داده شده است. هر مکان (i,j) در این مدل نشان‌دهنده آن است که گره در j امین برش زمانی از i امین تلاش خود در طی کردن بازه انتظار تعویق قرار دارد. احتمال مرتبط با

[1] Bianchi

رخداد برخورد در مدت زمان طی کردن پنجره انتظار تعویق با استفاده از روابط ریاضی از مدل ارائه شده استخراج شده است.



شکل ۳-۱ مدل مارکوف دوبعدی ارائه شده در مرجع [۳۷] به‌منظور نمایش مراحل مکانیزم انتظار تعویق

مدل ارائه شده به همراه محاسبات ریاضی مرتبط، با در نظر گرفتن تمام مراحل الگوریتم مانند مکانیزم دست تکانی RTS/CTS و موارد دیگر معیار توان گذردهی[1] در یک شبکه ایده آل بررسی شد. این معیار تحت شرایطی مانند تعداد ایستگاه‌های بی‌سیم، اندازه بسته‌های داده ردوبدل شده، طول پنجره اولیه انتظار تعویق و حداکثر اندازه پنجره انتظار تعویق بررسی شده است. با وجود جامع و کامل بودن مطالعه صورت گرفته در این تحقیق مواردی مانند فرض ایده آل بودن شبکه (نبود مشکل گره مخفی

[1] Throughput

و ...)، ثابت بودن مکان گره‌ها و بررسی تنها یک معیار (توان گذردهی) از مشکلات این تحقیق بوده است.

هه و همکاران[1] در مرجع [۳۸]، کارایی الگوریتم IEEE 802.11 DCF را در یک شبکه چندگامه با ارائه یک مدل تحلیلی بررسی نمودند. مدل ارائه شده مبتنی بر یک زنجیره مارکوف دو-بعدی جهت نشان دادن رفتار مکانیزم انتظار تعویق در این الگوریتم می‌باشد که از مرجع [۳۷] الهام گرفته شده است. از مدل ارائه شده به‌منظور استخراج احتمال انتقال[2] داده در کانال استفاده می‌شود که در این تحقیق در محاسبه معیار نرخ برخورد[3] بکار می‌رود. در زنجیره مارکوف ارائه شده تأثیر مسئله گره مخفی در آن بررسی شده است. همچنین در مدل ارائه شده تأثیر پارامترهای لایه فیزیکی که در لایه پیوند داده تأثیرگذار خواهند بود مانند شعاع تداخل و یا شعاع انتقال گره‌های بی‌سیم در نظر گرفته شده.. به‌منظور راحتی تحلیل در این تحقیق فرض است که گره‌ها در یک شبکه به‌صورت ثابت تحت توپولوژی مشبک[4] پراکنده شده‌اند.

گوانگ و همکاران[5] در [۳۹] اقدام به مطالعه رفتار یک گره متخاصم در لایه پیوند داده با استفاده از یک مدل مارکوف سه‌بعدی نمودند. در این تحقیق فرض شده است که گره متخاصم در این لایه تنها اقدام به کاهش اندازه طول پنجره انتظار تعویق خود با ضریب γ خواهد نمود. مدل ارائه شده در دو حالت استفاده از مکانیزم دست تکانی RTS/CTS و BA عمل می‌کند. نتایج به دست آمده با محاسبه مقدار توان گذردهی بر اساس مقادیر مختلف γ نشان داده شده است که در آن $0 \leq \gamma \leq 1$ می‌باشد. همچنین با استفاده از مدل ارائه شده یک الگوریتم اصلاحی برای مکانیزم انتظار تعویق ارائه شده که توسط آن نشان داده شده امکان عملکرد منفی گره‌های متخاصم بشدت کاهش می‌یابد. تأثیر مابقی

---

[1] He et al
[2] Transmission probability
[3] Packet collision
[4] Grid
[5] Guang et all

پارامترهای لایه پیوند داده در نتایج به دست آمده بررسی نشده است و همچنین فرض شده که گره‌های در جایگاه ثابتی قرار دارند. تحقیق ارائه شده توسط این نویسندگان در مرجع [۴۰] گسترش داده شد که در آن معیارهایی مانند متوسط تأخیر بسته‌ها[1] و عدالت[2] شبکه در ارسال بسته‌های داده بررسی شد و در تلاشی گسترده‌تر در [۴۱] بررسی مواردی چون نرخ ورود بسته‌ها به آن نیز اضافه شد. در مورد آخر نویسندگان اقدام به بررسی پارامترهایی مانند متوسط تأخیر بسته‌ها، عدالت، نرخ تحویل بسته و میزان توان گذردهی کل شبکه بر اساس تعداد ایستگاه‌های بی‌سیم و میزان ترافیک داده ورودی با استفاده از پروتکل پایه مکانیزم انتظار تعویق و روش اصلاحی خود نمودند. در هر آزمایش شدت حملات اعمالی با استفاده از قابلیت گره‌هایی نشان داده شده که می‌توانند طول پنجره انتظار تعویق خود را به‌اندازه ضریب γ کوتاه‌تر کنند. روش اصلاحی ارائه شده در اکثر آزمایش‌های انجام شده در این تحقیق دارای معیارهای بهتری نسبت به الگوریتم پایه در مقابل حملات برخوردار است.

مطالعات صورت گرفته قبلی تنها اقدام به بررسی حمله دست‌کاری طول پنجره انتظار تعویق نموده و راهی برای شناسایی و یا کاهش اثر گره متخاصم ارائه نمودند. رایا و همکاران[3] در [۴۲] بررسی جامع‌تری نسبت به انواع حملات لایه پیوند داده ارائه دادند. حملاتی مانند دست‌کاری طول بردار NAV، کوتاه کردن طول بازه DIFS و با افزایش زمان استاندارد ارسال داده در این تحقیق بررسی شد. در این مطالعه همچنین راهی جهت شناسایی و کاهش اثر این حملات ارائه شده است که به نام پروتکل DOMINO نام گرفته است. روش ارائه شده در شبیه‌ساز NS-2 پیاده‌سازی شده و نتایج تنها روی حمله کاهش سایز پنجره انتظار تعویق بر اساس ضریب آن (γ) بر اساس معیارهایی توان

[1] Average packet delay
[2] Fairness
[3] Raya et al

گذردهی و نرخ تشخیص نمایش داده شده است. با وجود مبتنی بر شبیه‌سازی بودن راهبرد ارائه شده در این تحقیق، در برخی موارد به جهت محاسبه مقادیر آستانه تشخیص از نتایج موجود در مدل مارکوف ارائه شده در [۳۷] نیز استفاده شده است.

کیاسانور و وایدیا[1] در [۴۳] راهی برای تشخیص و کاهش اثر حملات لایه پیوند داده با شناسایی گره‌های متخاصم و اعمال یک تابع جریمه به آن ارائه شده است. روش کار دارای یک مبنای تحلیلی بوده که در محیط NS-2 شبیه‌سازی شده است. معیارهای عدالت[2]، توان گذردهی و نرخ تشخیص در حالت عملکرد گره‌های متخاصم و یا بدون آن‌ها برای ارزیابی پروتکل ارائه شده محاسبه شده است. آزمایش‌ها بر اساس تعداد گره‌های متخاصم و مشروع انجام شده است.

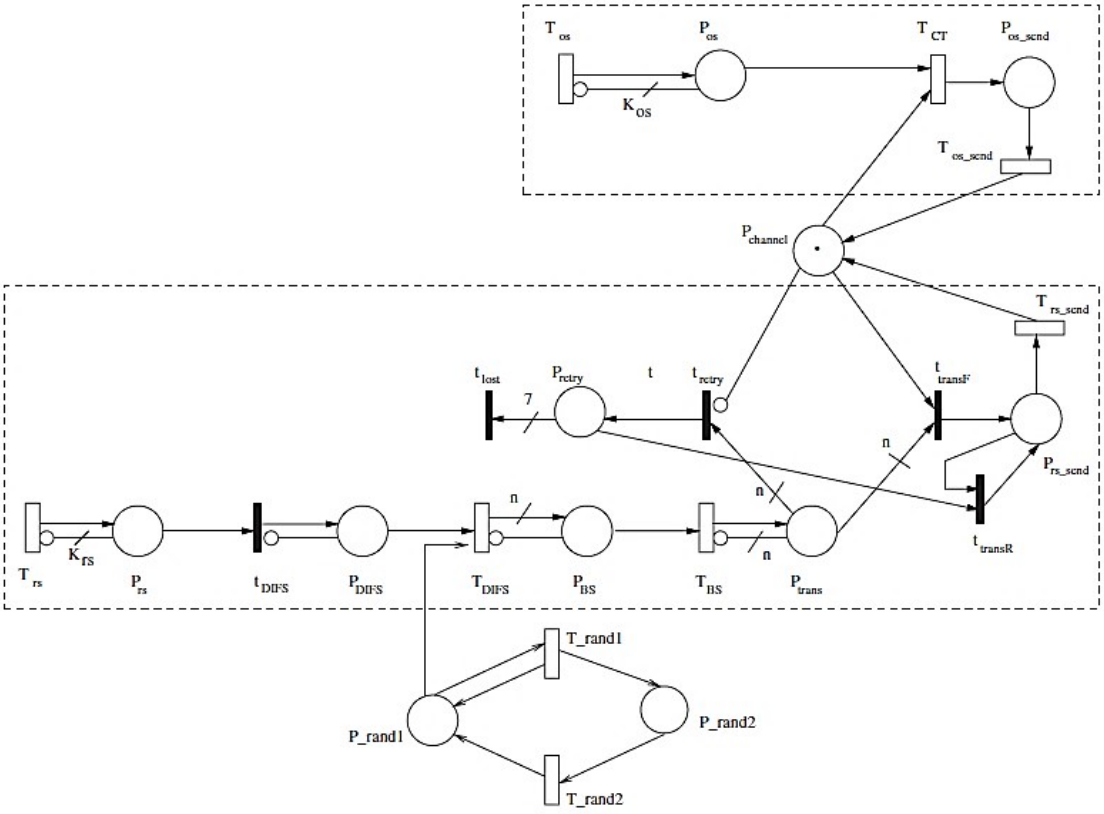
ونگ و چنگ[3] در [۴۴] ارزیابی از عملکرد پروتکل IEEE 802.11 DCF در یک کانال متراکم[4] ارائه دادند. ارزیابی ارائه شده که مبتنی بر یک مدل مارکوف الهام گرفته از [۳۷] می‌باشد با هدف مقایسه نتایج به دست آمده با کار ارائه شده توسط زیووا و آنتوناکوپولوس[5] [۴۵] تهیه شده است. نویسندگان این تحقیق ادعا نمودند که شرایط تعریف شده برای یک کانال متراکم در [۴۵] مناسب نبوده و با واقعیت فاصله دارد. نتایج بر اساس دو معیار توان گذردهی و تأخیر ارسال بر اساس دو مکانیزم دست تکانی RTS/CTS و BA محاسبه شده است. نتایج ارائه شده بر اساس مقادیر مختلف اندازه اولیه پنجره انتظار تعویق و اندازه بسته‌های داده محاسبه شده است. نویسندگان بهبود عملکرد پروتکل IEEE 802.11 DCF و ارائه یک مدل تحلیلی برای پروتکل بهبود داده شده را به‌عنوان کار آتی خود عنوان نمودند.

---

[1] Kyasanur and Vaidya
[2] Fairness
[3] Weng and Chen
[4] Busy medium
[5] Ziouva and Antonakopoulous

جایاپاروادی و همکاران [1]در سال ۲۰۰۷ برای اولین بار در [۴۶] اقدام به ارزیابی و تحلیل پروتکل IEEE 802.11 DCF با استفاده از مدل SRN به جهت قابلیت آن در مدل‌سازی فرآیندهای همگام نمودند. مدل ارائه شده که در شکل ۳-۲ نشان داده شده است سعی در نشان دادن تمامی عملیات صورت گرفته در این پروتکل داشته است که البته در نشان دادن بسیاری از این عملیات موفق نبوده است. از جمله، می‌توان به عملیات مربوط به مکانیزم دست تکانی و یا عملیات مربوط به صدور تأییدیه دریافت داده (ACK) و یا سپری شدن زمان استاندارد و عدم دریافت تأییدیه (timeout). نویسندگان در این تحقیق سعی نمودند که اثر تعامل یک گره با گره‌های دیگر را نیز در این مدل نشان دهند که در اینجا از تکنیک لایه‌بندی[2] استفاده نمودند. همچنین ایده استفاده تنها یک گره از کانال در اینجا توسط یک مکان با بیشینه تنها یک نشانه نمایش داده شده است.

[1] Jayaparvathy et al
[2] Folding



شکل ۳-۲ مدل SRN ارائه شده در مرجع [۴۶] جهت ارزیابی عملکرد پروتکل IEEE 802.11 DCF

در تحلیل مدل ارائه شده از تکنیک‌های تحلیل صف (M/G/1) و ارزیابی مقایسه‌ای با شبیه‌ساز NS-2 استفاده شده است. آزمایش‌ها بر اساس پارامترهایی مانند اندازه بسته داده و نرخ ارسال داده برای محاسبه معیارهای متوسط زمان انتظار و توان گذردهی سیستم ارائه شده است که حاکی از تطابق مقادیر به دست آمده از مدل تحلیلی و شبیه‌ساز NS-2 داشته است. همان‌طور که ذکر شد به بسیاری از مکانیزم‌های موجود در پروتکل IEEE 802.11 DCF و همچنین مسائلی مانند گره مخفی در این مدل توجهی نشد. همچنین نویسندگان این تحقیق مشخص نکردند که سناریو آزمایش شده توسط آن‌ها در یک محیط حرکتی پویا بوده است یا خیر؟

یونس و توماس[1] در سال ۲۰۱۱ در [۴۷] با الهام از تحقیق صورت گرفته در [۴۶] اقدام به تحلیلی عملکرد پروتکل IEEE 802.11 DCF در قبال اثر گره‌های مخفی نمودند. مدل ارائه شده مبتنی بر دو مدل SRN یکی برای مدل کردن عملیات صورت گرفته در یک گره و دیگری برای مدل کردن تعامل میان گره‌های موجود در یک فضای همسایگی می‌باشد. همانند [۴۶] در اینجا نیز از روش ارزیابی مقایسه‌ای برای اثبات صحت مدل ارائه شده استفاده شده که در آن مقادیر به دست آمده از مدل تحلیلی به ازای معیارهای متوسط زمان انتظار و نرخ توان گذردهی با مقادیر به دست آمده از شبیه‌ساز NS-2 مقایسه شده است. کلیه نتایج روی مقادیر مختلف اندازه بسته داده و نرخ ارسال آن و تعداد گره‌های موجود در ناحیه مخفی بررسی شده‌اند. مدل ارائه شده از یک سناریو ثابت با تعداد گره‌های مشخص استفاده می‌کند که امکان کارکرد آن در یک محیط پویا یا گره‌های متحرک را ناممکن می‌سازد. همچنین فرض شده که تمام گره‌ها مشروع بوده و از قوانین پروتکل IEEE 802.11 DCF تبعیت می‌کنند. درنتیجه‌گیری دیگری در این تحقیق نشان داده شده که با افزایش پارامترهایی مانند تعداد گره‌های همسایگی و یا تعداد گره‌های ناحیه مخفی روی تعداد وضعیت‌های ایجادشده در مدل مارکوف ایجادشده برای اجرای مدل SRN تأثیر زیادی داشته و مقدار آن را به‌طور قابل‌توجهی اضافه می‌کند. با این حال، زمان استخراج معیارهای کارایی از دل مدل تحلیلی در مقایسه با یک سناریو مشابه در شبیه‌ساز NS-2 کاملاً ناچیز می‌باشد.

مارسی و همکاران (۲۰۰۹) در [۴۸] نیز سعی در ارزیابی کارایی پروتکل IEEE 802.11 b با استفاده از مدل‌سازی شبکه پتری داشته‌اند. نویسندگان در این تحقیق ابتدا اقدام به بررسی و مطالعه کلاس‌های مختلف پتری و توانایی آن در مدل‌سازی پروتکل‌های ارتباطی نمودند و سپس سعی در

[1] Younes and Thomas

مدل‌سازی با استفاده از کلاس شبکه پتری شئ گرا[1] نمودند. نتایج بر اساس تعداد گره‌ها روی معیارهای نرخ ازدحام[2]، زمان ارسال و توان گذردهی ارزیابی شده‌اند که به ازای معیار توان گذردهی با مقادیر به دست آمده از NS-2 نتایج مقایسه شده‌اند. البته به رابطه‌ای برای نحوه استخراج معیارها از مدل در این تحقیق اشاره‌ای نشده است. موکداد و همکاران[3] نیز در سال ۲۰۱۲ در [۴۹] با ارائه یک روش تحلیلی با استفاده از مدل مارکوف و شبکه پتری رنگی اقدام به ارائه و ارزیابی یک پروتکل مبتنی بر کیفیت برای لایه پیوند شبکه‌های سنسوری داده نمودند.

۳-۲- ارائه مدل تحلیلی جهت ارزیابی لایه شبکه:

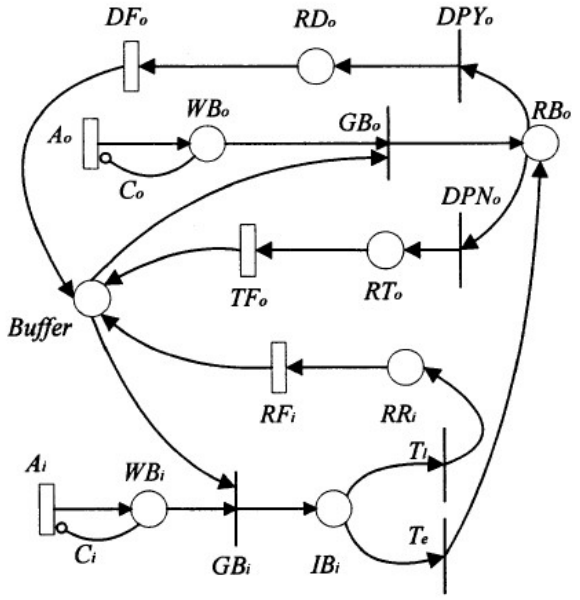
همان‌طور که در بخش ۲-۱-۲-۱ توضیح داده شد، لایه شبکه در شبکه‌های موردی سیار به جهت گستردگی عملیات موجود در آن از پیچیدگی بالاتری نسبت به لایه پیوند داده برخوردار است. به همین جهت مدل‌سازی مجموعه فعالیت‌های موجود در یک پروتکل مسیریابی لایه شبکه دارای سطح انتزاع و احتمال بالاتری نسبت به لایه پیوند داده می‌باشد. به طبع مجموعه تحقیقات صورت گرفته در مدل‌سازی عملیات لایه شبکه به نسبت لایه پیوند داده بسیار کمتر می‌باشد.

به‌عنوان اولین تلاش قابل‌توجه، ژانگ و ژو[4] در ۲۰۰۳ در [۵۰] اقدام به تحلیل عملکرد سطح بالای شبکه‌های موردی سیار در با استفاده از مدل پتری GSPN نمودند. در مدل ارائه شده توسط این نویسندگان که در شکل ۳-۳ نشان داده شده است فرآیند جریان داده ورودی به یک گره و خروجی از یک گره مدل شده است. نویسندگان در این تحقیق عنوان نمودند که اندازه‌گیری معیارهای ارزیابی یک گره در شبکه می‌تواند نمودی از معیارهای ارزیابی کل شبکه باشد. مشکل اصلی در این مقاله ساده‌انگاری محاسبه مقادیری مانند احتمال مقصد داده بودن گره جاری، احتمال مرتبط با ارسال

---

[1] Object oriented petri net
[2] Collision rate
[3] Mokdad et al.
[4] Zhang and Zhou

موفقیت‌آمیز داده به گره بعدی، نرخ داده ورودی به گره جاری، متوسط تعداد گام طی شده تا مقصد و موارد دیگر در مدل می‌باشد. صحت مدل ارائه شده با مقایسه مقادیر استخراج شده از آن به ازای معیارهای نرخ تحویل بسته، توان گذردهی و تأخیر ارسال داده با مقادیر به دست آمده از NS-2 ارزیابی شده است.



شکل ۳-۳ مدل SPN ارائه شده در مرجع [۵۰] جهت ارزیابی لایه شبکه

جیانگ[1] و همکاران (۲۰۱۴) در [۲۵] روشی برای جلوگیری از ارسال سیل‌آسای بسته‌های RREQ پیشنهاد داده که سبب کاهش اثر حمله ارسال سیل آسا به میزان قابل‌توجهی خواهد شد. نویسندگان در این تحقیق روش ارائه شده توسط خود را با استفاده از مدل شبکه پتری پایه مدل‌سازی و ارزیابی نمودند. در این تحقیق نشان داده شده که روش پیشنهادی به میزان قابل‌توجهی سبب بالا رفتن عمر شبکه حتی با اضافه کردن تعداد گره‌های مهاجم خواهد شد. هوآنگ و ژو[2] (۲۰۱۲) در [۵۱] با

[1] Jiang et al.
[2] Huang and Zhou

استفاده از مدل شبکه پتری رنگی اقدام به ارائه مدلی برای مقابله با حمله سیاه‌چاله در شبکه‌های توری[1] با استفاده از شبکه پتری رنگی نمودند. نویسندگان در این مقاله راهبردی برای تشخیص صحت عملکرد الگوریتم، ارائه نکردند. همچنین مدل ارائه شده قابلیت تطبیق با یک سناریو قابل پیاده‌سازی را نیز ندارد. بیانچینی و پیزوتیلو[2] در [۵۲] با استفاده از مدل شبکه پتری رنگی سعی در بررسی خصوصیات پروتکل مسیریابی DSR برای پیش‌بینی رفتار این الگوریتم نمودند. این کار به‌صورت دقیق‌تر و با جزئیات بیشتری توسط ژیونگ و همکاران[3] در [۵۳] و دوانگان و چوبی[4] در [۵۴] انجام شده است. متأسفانه سه تحقیق اخیر فاقد ساز و کار لازم جهت ارزیابی یک سناریو مشخص از شبکه می‌باشد و تنها در حد ارائه یک مدل است. وانگ و همکاران[5] نیز در [۵۵] با استفاده از مدل مارکوف پیوسته روشی را برای ارزیابی کارایی پروتکل مسیریابی DSR ارائه نمودند. روش ارائه شده مبتنی بر مبانی ریاضی قوی و مستدل بوده و از آن برای محاسبه معیارهایی مانند محاسبه تابع احتمال فاصله ارسال، احتمال پیدا شدن مقصد در یک تقاضای مسیر با محدودیت گام، فرکانس بازیابی مسیر و مدت زمان متوسط معتبر بودن مسیر استفاده شده است. متأسفانه در این تحقیق نیز تحلیل جامعی برای آزمایش روش، ارائه نشده (به‌جز معیار متوسط فاصله) و تنها به ذکر روابط ریاضی استخراج شده پرداخته شده است.

۳-۳- ارائه مدل تحلیلی برای دیگر جنبه‌های شبکه‌های موردی سیار

علاوه بر عملکرد لایه‌های استاندارد در شبکه‌های موردی سیار، موارد دیگری نیز در این شبکه‌ها وجود دارد که نیاز به ارائه یک ارزیابی از آن وجود دارد. ازجمله این موارد می‌توان ارزیابی پایداری اتصال

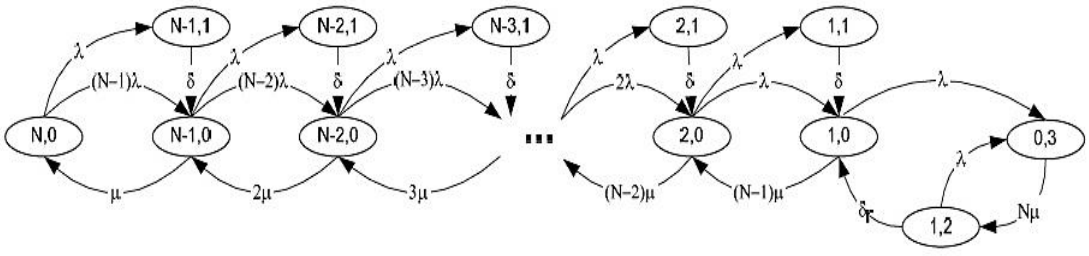
---

[1] Mesh network
[2] Biachini and Pizzutilo
[3] Xiong et al.
[4] Dewangan and Choubey
[5] Wang et al.

اتصال بین گره‌های بی‌سیم، پیش‌بینی درجه اتصال بین گره‌های بی‌سیم و ارزیابی قابلیت اعتماد شبکه نام برد.

تراجانو و همکاران[1] (۲۰۰۲) در [۵۷] یک مدل مبتنی بر مارکوف پیوسته برای ارزیابی قابلیت اتصال در شبکه‌های موردی سیار ارائه نمودند که در شکل ۳-۴ نشان داده شده است. مدل ارائه شده به همراه روابط ریاضی نشانگر نرخ خروج از ناحیه مشترک بین گره‌های همسایه و یا ورود به آن به‌منظور ارزیابی قابلیت دسترسی استفاده می‌شود. نویسندگان این تحقیق با فرض وجود N گره در یک فضای همسایگی احتمال و نرخ خروج هریک از این N گره را با استفاده از روابط ریاضی محاسبه نموده و درنهایت میزان در دسترس بودن مسیر را برای یک ارتباط یک گامه محاسبه نموده و از آن برای محاسبه در دسترس بودن یک مسیر n-گامه استفاده کردند. در مدل ارائه شده این تحقیق هیچ توجهی به نوع پروتکل مسیریابی شبکه و تأثیر آن نشده است.

چن و همکاران[2] (۲۰۰۴) در [۵۷] با استفاده از یک مدل مارکوف پیوسته دو-بعدی مشابه با آنچه در [۵۶] ارائه شده اقدام به ارائه راهبرد کمی جهت ارزیابی بقای یک شبکه[3] موردی سیار نمودند. بقای یک شبکه در این تحقیق به توانایی شبکه در ادامه فعالیت خود در زمان و یا بعد از رخداد خطا تعریف شده است که به‌صورت کمّی، به مدت زمان رخداد خطا و تأثیر آن در شبکه مقداردهی می‌شود.



[1] Trajanov et al.
[2] Chen et al.
[3] Network survivability

شکل ۳-۴ مدل مارکوف پیوسته استفاده شده در مرجع [۵۶] جهت محاسبه میزان در دسترس بودن مسیر

روش تحلیلی ارائه شده، هم به تحلیل حالت پایدار و هم حالت گذرای سیستم پرداخته است که ادعاشده می‌تواند برای تحلیل پایداری سیستم‌های دیگر به‌جز شبکه‌های موردی سیار نیز استفاده شود.

سونگ و همکاران[1] (۲۰۱۲) در [۵۸] به موضوع پایداری اتصال گره‌ها در شبکه‌های موردی سیار پرداختند و سعی نمودند تا یک مدل ریاضی برای تخمین پایداری اتصال گره‌ها ارائه نمایند. مدل ارائه شده هم برای سناریوهای ساکن و هم سناریوهای با گره‌های متحرک مناسب می‌باشد که بر اساس تغییرات اتصال گره‌ها پایداری آن را تخمین می‌زند. در این تحقیق ادعا شده که روش ارائه شده را می‌توان بدون نیاز به هیچ سخت‌افزار اضافی در لایه شبکه[2] شبکه‌های موردی سیار و تحت هر پروتکل مسیریابی پیاده‌سازی کرد و بر اساس آن نیز یک مدل مسیریابی پیشنهاد شده که کارایی آن بیشتر از پروتکل‌های مسیریابی مرسوم است که از موضوع پایداری اتصال گره‌ها در تعیین مسیر بهینه استفاده نمی‌کنند. کلیه آزمایش‌ها در این تحقیق بر اساس مدل حرکتی Random Walk بوده که در گره‌هایی با سرعت‌های متفاوت بررسی شده است.

یونس و توماس[3] (۲۰۱۲) در [۵۹] اقدام به ارائه یک مدل شبکه پتری به‌منظور مطالعه قابلیت دسترسی مسیر[4] در یک شبکه موردی سیار نمودند. در مدل ارائه شده با کمک روابط ریاضی تأثیر پارامترهایی چون محدوده انتقال گره، ابعاد شبکه، نرخ انتقال داده و نوع پروتکل مسیریابی را با استخراج معیارهایی چون احتمال از دست رفتن مسیر و نرخ از دست رفتن مسیر ارزیابی شده است. مدل پتری ارائه شده که الهام گرفته از مدل‌های مارکوف ارائه شده در [۵۷] می‌باشد، با محاسبه تعداد گام لازم جهت دستیابی به مقصد (n)، از n قطعه مدل پتری تشکیل شده است. در هر قطعه پتری

[1] Song et al
[2] Network layer
[3] Younes and Thomas
[4] Path connection availability

نرخ خروج گره همسایه‌ای که به‌عنوان گره بعدی در مسیر قلمداد می‌شود به همراه نرخ بازیابی گره دیگری به‌عنوان گره جایگزین محاسبه شده است. در مدل مذکور به نوع پروتکل مسیریابی شبکه توجه شده و بر اساس دو پروتکل AODV و DSR طراحی شده است. نتایج بر اساس این دو نوع پروتکل مسیریابی، ابعاد شبکه و نرخ ارسال داده در شبکه برای محاسبه معیارهای فرکانس خرابی و بازیابی مسیر، نرخ در دسترس بودن شبکه محاسبه شده است.

کستین و همکاران[1] در [۶۰] با استفاده از کلاس شبکه پتری توسعه‌یافته به بررسی مسئله پایداری اتصال گره‌ها در یک شبکه بی‌سیم پرداختند. در مدل ارائه شده به جنبه‌های از موارد تأثیرگذار در قابلیت اعتماد شبکه‌های بی‌سیم پرداخته شده است. موارد بررسی شده شامل اثرات محوشدگی[2] و تداخل سیگنال، وجود مانع و شرایط آب و هوایی می‌باشد. کارایی یک شبکه بی‌سیم با استفاده از این مدل با استخراج چهار معیار از آن (نرخ تحویل بسته، متوسط تعداد گام از مبدأ به مقصد، ترافیک نسبی شبکه و تأخیر انتها به انتها) به ازای مقادیر مختلفی از شعاع محدوده انتقال و موارد دیگر ارزیابی شده است. پویان و یداله زاده طبری نیز در [۶۱] اقدام به ارائه مدلی جهت اندازه‌گیری قابلیت اعتماد در شبکه‌های بی‌سیم سیار با استفاده از روش محاسبه مونت‌کارلو نمودند. قابلیت اعتماد در این تحقیق به احتمال رسیدن بسته داده از مبدأ به مقصد تفسیر شده است که با روش ارائه شده در مدت زمان کوتاهی قابل‌محاسبه خواهد بود.

---

[1] Kostin et al
[2] Fading

فصل ۴– روش تحقیق

همان‌طور که در فصل ۱ بیان شد هدف از این پایان‌نامه مدل‌سازی و ارزیابی شبکه‌های موردی سیار در مقابل حملات با استفاده از تکنیک مدل‌سازی شبکه پتری می‌باشد. با توجه به پیچیدگی‌های موجود در عملکرد پروتکل های موجود در شبکه‌های موردی سیار از مدل شبکه پتری تصادفی مبتنی بر پاداش برای این مدل‌سازی استفاده شده است. همانطور که در فصل‌های ۱ و ۲ توضیح داده شد انتخاب این نوع از شبکه پتری به جهت توانایی های آن در مدل سازی فعالیت های همروند، انتخاب فعالیت ها، پردازش موارد استثناء، وجود امکاناتی از قبیل کمان‌های بازدارنده، توابع محافظتی و ابزارهای مناسب مبتنی بر پاداش جهت ارزیابی سیستم بوده است. مدل سازی صورت گرفته با تمرکز روی دو لایه پیوند داده و شبکه انجام شده است. این امر در درجه اول به این علت می باشد که مهم‌ترین فعالیت‌های صورت گرفته در یک شبکه موردی سیار مربوط به دو لایه پیوند داده و شبکه است و همچنین غالب حملات تعبیه شده در این شبکه‌ها نیز مربوط به این دو لایه می باشد. لذا در بخش‌های ۴-۱ و ۴-۲ به ارائه مدل تحلیلی شبکه‌های موردی سیار به ترتیب برای لایه‌های پیوند داده و شبکه پرداخته شده است. همچنین در تلاشی دیگر به ارائه یک پروتکل مسیریابی امن بر اساس پروتکل مسیریابی AODV با الهام از مدل پتری فازی پرداخته شده که در بخش ۴-۳ توضیح داده شده است.

۴-۱- مدل ارائه شده جهت لایه انتقال داده

در بررسی کارایی لایه انتقال داده باید به این نکته توجه داشت که عملکرد این لایه درواقع در قالب تعدادی گره معنی پیدا می‌کند که برای دستیابی به کانال مشترک انتقال داده با هم رقابت می‌کنند. بنابراین با در نظر گرفتن شبکه‌ای شامل M گره متحرک که به‌طور متوسط دارای N گره در هر همسایگی می‌باشد تنها کافی است تا مدل ارائه شده به بررسی عملکرد آن N گره همسایه که برای دستیابی به کانال باهم رقابت می‌کنند، توجه شود. از آنجائی که ما در این قسمت قصد بررسی عملکرد پروتکل لایه انتقال IEEE 802.11 DCF را در مقابل حملات داریم،

لازم است تا رفتار غیرمعمول گره‌های متخاصم را علاوه بر رفتار متعارف گره‌های مشروع و همچنین نحوه تعامل و برخورد آن‌ها با یکدیگر را مدل کنیم. برای مدل کردن رفتار متعارف گره‌ها در لایه انتقال داده لازم است مواردی چون مکانیزم تعویق، مکانیزم دست تکانی چهار مرحله‌ای RTS/CTS، تعیین مقدار تایمر NAV و بازه انتظار DIFS و SIFS جهت پایش کانال در مدل ارائه شده لحاظ شود. همچنین لازم است برای گره‌های متخاصم تمام این موارد با اعمال تغییرات موردنظر این گره‌ها در مدل ارائه شده گنجانده شود. به‌عنوان یک مشکل قابل‌توجه در ارتباط گره‌ها در لایه انتقال داده مسئله گره‌های مخفی که در فصل ۲ درباره آن توضیح داده شده ازجمله مواردی است که لازم است در مدل ارائه شده به آن توجه شود. با وجوداینکه هدف از این تحقیق بررسی اثر این مشکل در عملکرد گره‌های بی‌سیم در لایه انتقال داده نیست، اما با توجه به نقش تأثیرگذار آن درنتیجه به دست آمده در شاخص‌های کارایی گره‌ها در این لایه، لازم است تا در مدل ارائه شده به آن توجه کامل شود.

شکل ۲-۷ شبکه فرضی شامل N گره که در همسایگی هم قرار دارند را نشان می‌دهد که در کنار آن‌ها N_m گره متخاصم قرار دارند. N گره مشروع به‌طور طبیعی سعی می‌کنند با استفاده از قوانین پروتکل IEEE 802.11 DCF ارسال داده خود را در کانال مشترک هماهنگ کنند. ارتباط میان این گره‌ها ممکن است از طرف N_m گره متخاصم و همچنین N_{cs} گره موجود در ناحیه مخفی دچار اختلال شود. چراکه گره‌های متخاصم با تغییر در پارامترهای پروتکل لایه انتقال داده سعی می‌کنند شانس بیشتری را برای تصاحب کانال از انتقال داده از آن خود کنند و همچنین ارسال داده از طرف N_{cs} گره موجود در ناحیه مخفی ممکن است با ارسال داده از طرف گره‌های موجود در همسایگی برخورد داشته باشد. توضیحات لازم برای حملات لایه انتقال داده در بخش ۲-۱-۲-۵ ارائه شده است.

نکته مهم دیگری که در ارائه مدل لازم است توجه شود آن است که ارائه آن در غالب یک مدل یکپارچه ممکن است سبب بروز مشکل انفجار حالت‌ها در ارزیابی آن شود. بنابراین برای جلوگیری از این مشکل بر اساس تکنیک تجزیه سازی، چهارچوب مدل ارائه شده بر اساس دو مدل جداگانه ارائه خواهد. یک مدل جهت توصیف رفتار پایه‌ای پروتکل لایه انتقال داده IEEE 802.11DCF و یک مدل نیز جهت توصیف ارتباط میان گره‌ها. در اینجا، مدل اول، مدل **عملکرد جزئی گره‌ها** و دومی نیز **مدل برهم‌کنش گره‌ها** نامیده می‌شود. با ارائه روابط ریاضی جهت محاسبه تعداد گره‌های موجود در هر همسایگی، مدل ارائه شده به‌صورت پویا توانایی تطبیق با هر مقیاس از شبکه، مشخصه و تعداد گره را دارد. در ارائه این روابط فرض شده که گره‌ها از مدل حرکتی Random Way Point(RWP) [۶۲] تبعیت می‌کنند.

۴-۱-۱-مدل SRN جزئی هر گره

این مدل که در شکل ۴-۱ نشان داده شده است برای توصیف عملکرد پایه‌ای پروتکل IEEE 802.11 DCF در هر گره ارائه شده است. برای ارسال داده در کانال، یک گره در ابتدا نیازمند تخصیص یک فضای بافر خالی در خود می‌باشد. از آنجائی که یک گره در هر لحظه امکان ارسال تنها یک بسته داده را دارد، بنابراین مقدار K در مکان P_{Buff} که برای این منظور در نظر گرفته شده به عدد یک تنظیم خواهد شد. به‌مجرد دریافت داده از لایه بالاتر و اختصاص بافر به آن لایه پیوند داده آماده ارسال آن در کانال می‌شود. گذار زمان‌دار T_{DR} دریافت داده از لایه بالاتر (شبکه) را نشان می‌دهد. نرخ فعالیت این گذار برابر با توان گذردهی مدل SRN در نظر گرفته شده جهت لایه شبکه[1] است که در بخش ۴-۲ معرفی خواهد شد. همان‌طور که در بخش ۲-۱-۳ بیان شد هر گره به تعداد دفعات محدودی اجازه باز ارسال داده خود را در کانال دارد. به همین منظور

[1] Network layer

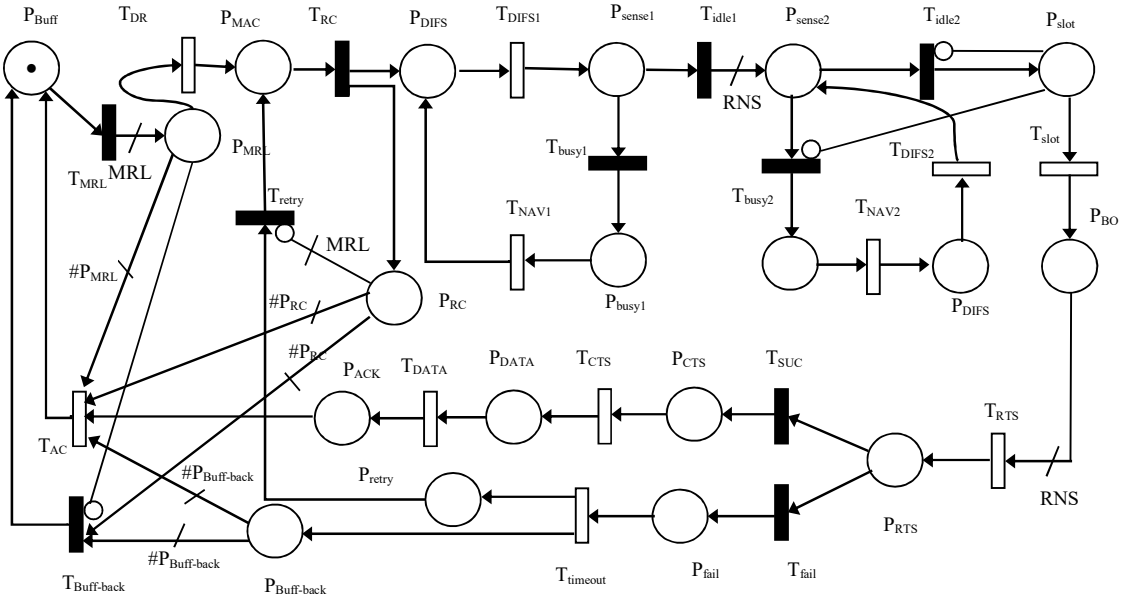
گذار T_{MRL} با هر بار تخصیص بافر تعداد MRL نشانه را در مکان P_{MRL} قرار می‌دهد که با هر بار اجرای گذار T_{DR} یک نشانه مصرف می‌شود. این کار تا زمانی که به یک ارسال موفقیت‌آمیز از ارسال داده و یا آنکه به بیشینه تعداد دفعات مجاز تلاش برای ارسال برسیم (تمام نشانه‌ها تمام شود) ادامه پیدا می‌کند. گذار T_{RC} نشان‌دهنده یک ارسال مجاز برای داده است. مکان و گذار P_{DIFS} و T_{DIFS} برای مدل کردن بازه انتظار DIFS جهت پایش کانال به‌منظور اطمینان از آزاد بودن آن قبل از ارسال بسته کنترلی RTS، ایجاد شده است. زمان لازم جهت فعالیت گذار T_{DIFS} از استاندارد موجود در پروتکل IEEE 802.11 DCF استخراج شده است. دو پیش آمد ممکن از این فرآیند که همان آزاد بودن و یا نبودن کانال در مدت زمان پایش DIFS می‌باشد توسط ساختار انتخاب مبتنی بر دو گذار آنی T_{idle1} و T_{busy1} نشان داده شده است. احتمال مرتبط با هریک از این دو پیشامد (α برای T_{busy1} و α-۱ برای T_{idle1}) از مدل برهم‌کنش گره‌ها استخراج خواهد شد.

درصورتی‌که کانال در این مدت مشغول باشد، گره بار دیگر کانال را به مدت DIFS بعد از تمام شدن تایمر NAV پایش می‌کند. به‌مجرد آزاد دیدن کانال در بازه زمانی DIFS، گره بسته کنترلی RTS را می‌تواند در کانال ارسال کند. اما، همان‌طور که در بخش ۲-۱-۳ بیان شد گره در این حالت ارسال بسته RTS را به اندازه پنجره انتظار تعویق که بر اساس رابطه ۲-۱ به دست می‌آید، به تعویق می‌اندازد. مشخصه RC در این رابطه بر اساس تعداد نشانه موجود در مکان P_{RC} به دست می‌آید که اندازه آن (تعداد برش‌های زمانی) در اینجا توسط RNS مشخص شده و به مکان P_{sense2} وارد می‌شود. در ابتدای هر برش زمانی و قبل از گذراندن آن، گره کانال را به‌منظور اطمینان از آزاد بودن آن پایش می‌کند. گره این کار را برای تمام برش‌های زمانی پنجره انتظار تعویق انجام می‌دهد. برای هر برش زمانی این احتمال وجود دارد که کانال آزاد و یا مشغول باشد که این مورد توسط یک ساختار انتخاب توسط دو گذار آنی T_{idle2} و T_{busy2} نشان داده شده است.

احتمال مرتبط با هریک از این دو پیشامد (α برای T_{busy2} و α-۱ برای T_{idle2}) همانند T_{idle2} و T_{busy2} و برابر با آن می‌باشد که از مدل برهم‌کنش گره‌ها استخراج خواهد شد. در صورت مشغول بودن کانال در ابتدای هر برش، گره با ثبت تعداد برش‌های زمانی باقیمانده، ابتدا باید تایمر NAV را تنظیم و آن را طی کند. سپس با طی کردن بازه انتظار DIFS، دوباره کانال را از ابتدای برش زمانی سپری‌شده، پایش می‌نماید.

سازوکار لازم برای انجام این کار توسط گذارهای زمان‌دار T_{NAV2} و T_{DIFS2} نشان داده شده که همانند T_{NAV2} و T_{DIFS2} زمان لازم برای فعالیت آن از استاندارد موجود در پروتکل IEEE 802.11 DCF استخراج شده است. هر گره با شنیدن پیغام RTS، تایمر NAV خود را به اندازه زمان لازم برای دریافت یک بسته CTS، یک بسته داده و یک پیغام ACK تنظیم می‌کند. بنابراین مدت زمان فعال شدن گذار T_{NAV} معادل رابطه ۴-۱ خواهد بود.

$$T_{NAV} = T_{CTS} + T_{DATA} + T_{ACK} \qquad (۱-۴)$$



شکل ۴-۱ مدل SRN جزئی گره

گذار T_{slot} نشان‌دهنده مدت زمان لازم جهت گذراندن یک برش زمانی[1] است. کمان بازدارنده بین مکان P_{slot} و گذارهای آنی T_{idle2} و T_{busy2} سبب می‌شود تا زمانی که نشانه‌ای منتظر فعال شدن گذار T_{slot} است، هیچ‌کدام از آن‌ها اجرا نشوند. این کار تضمین می‌کند تا قبل از اتمام برش زمانی جاری، برش زمانی جدیدی آغاز نشود. با پایان یافتن تعداد برش‌های زمانی پنجره انتظار تعویق و ذخیره کل تعداد RNS نشانه در مکان P_{BO}، گذار T_{RTS} قابلیت اجرا پیدا می‌کند. زمان فعالیت گذار T_{RTS} نیز بر اساس استاندارد IEEE 802.11 DCF استخراج خواهد شد. زمان لازم برای اجرای این گذار برابر زمان لازم جهت ارسال سرآمد بسته RTS و زمان لازم جهت ارسال خود بسته RTS می باشد. لازم به ذکر است که پروتکل IEEE 802.11 DCF بسته‌های سرآمد را با سرعت پایین‌تری نسبت به بسته‌های کنترلی و داده ارسال می‌کند. بنابراین رابطه زمان فعالیت گذار T_{RTS} به‌صورت زیر خواهد بود.

$$T_{RTS} = \frac{phH}{B1} + \frac{RTS}{B2} \qquad (۲-۴)$$

آغاز مرحله فرستادن بسته کنترلی RTS، درواقع آغاز عملیات دست تکانی چهارمرحله ای RTS/CTS می‌باشد. شکست در هر یک از این مراحل، کل فرآیند را دچار اختلال می‌کند. در اینجا احتمال موفقیت و یا عدم موفقیت در کل فرآیند RTS/CTS به‌صورت یکجا توسط ساختار انتخاب توسط دو گذار آنی T_{succ} (β) و T_{fail} (۱-β) نشان داده شده است. T_{fail} درواقع نشان‌دهنده آن است که در یکی از مراحل ارسال بسته‌های کنترلی در کانال برخورد رخ داده است و T_{succ} نیز نشان‌دهنده موفقیت در کل فرآیند است. احتمال مرتبط با این دو گذار از محاسبات موجود در مدل برهم‌کنش گره‌ها محاسبه می‌شود. با هر بار فعال شدن گذار T_{fail}، گره به اندازه مدت زمان timeout جهت دریافت پاسخ صبر می‌کند. مدت زمان timeout برابر زمان

[1] slot

لازم جهت ارسال یک بسته داده و انجام کامل یک مرحله دست تکانی چهارمرحله ای RTS/CTS است. البته بازه انتظار timeout در هریک از مراحل مکانیزم دست تکانی RTS/CTS ممکن است رخ دهد. اما در اینجا فرض را بر این گذاشته می‌شود که گره‌ها مشکلی در دریافت بسته کنترلی CTS نداشته باشند. بنابراین زمان لازم جهت فعالیت گذار $T_{timeout}$ بر اساس رابطه ۴-۳ محاسبه خواهد شد.

$$T_{timeout} = T_{DATA} + T_{ACK} \qquad (۳-۴)$$

با هر بار اجرای گذار $T_{timeout}$ که نشان دهنده ناموفق بودن یک تلاش مجاز برای ارسال داده در کانال است باید مشخص شود که گره برای تلاش بعدی مجاز می‌باشد یا خیر. این کار ازطریق مجموعه ساختاری P_{retry}، T_{retry} و کمان بازدارنده بین P_{RC} و T_{retry} انجام می شود. اختصاص وزن MRL به این کمان تضمین می کند که در صورت نرسیدن تعداد تلاش انجام شده (تعداد نشانه در مکان P_{RC}) به مقدار MRL انجام این کار مجاز باشد. همچنین با هر بار اجرای گذار $T_{timeout}$ یک نشانه در مکان $P_{Buff\text{-}back}$ قرار می گیرد که برای رصد کردن تعداد تلاش‌های ناموفق جهت ارسال داده در کانال تعبیه شده است. با جمع شدن MRL تعداد نشانه در مکان $P_{Buff\text{-}back}$ و همچنین خالی شدن P_{MRL}، گذار $T_{Buff\text{-}back}$ امکان فعال شدن را پیدا می‌کند. در این صورت، گره مجدداً در صف انتظار جهت ارسال داده قرار می‌گیرد. با فعال شدن گذار $T_{Buff\text{-}back}$ کل نشانه‌های مکان P_{RC} خالی شده و یک نشانه به مکان P_{Buff} اضافه شده تا شرایط اولیه برای ارسال داده توسط یک گره جدید فراهم شود. در صورت موفقیت‌آمیز بودن مکانیزم دست تکانی RTS/CTS مراحل آن توسط گذارهای T_{CTS}، T_{DATA} و T_{ACK} انجام خواهد شد که زمان‌های آن نیز مطابق با استاندارد IEEE 802.11 DCF توضیح داده شده در بخش ۲-۱-۳-۱ محاسبه خواهد شد. به‌طورکلی زمان فعال شدن هریک از این گذارها برابر زمان لازم جهت ارسال بسته سرآمد فیزیکی، زمان لازم جهت ارسال خود بسته DATA، CTS و یا ACK، بازه انتظار SIFS (τ_{SIFS})

جهت اطمینان از خالی بودن کانال، زمان تشخیص نوع سیگنال (τ_{CCA}) و زمان تبدیل وضعیت از حالت فرستنده به گیرنده و بالعکس (τ_{RxTx}) می‌باشد.

جدول ۴-۱ لیست گذارهای زمان‌دار و آنی استفاده شده در مدل جزئی گره‌ها

زمان فعالیت یا احتمال اجرا	توضیح	نوع	نام گذار
$1/\lambda$	نرخ دریافت داده از لایه بالاتر	زمان‌دار	T_{DR}
---	به تعداد MRL نشانه در P_{MRL} قرار می‌دهد که معرف حداکثر تعداد تلاش گره جهت ارسال داده در کانال است.	آنی	T_{MRL}
τ_{DIFS}	گذار زمان‌دار معرف پایش کانال به مدت زمان DIFS قبل از ارسال داده توسط گره	زمان‌دار	T_{DIFS1}, T_{DIFS2}
α(از مدل برهم‌کنش گره‌ها استخراج می‌شود)	گذار آنی معرف احتمال **آزاد** بودن کانال بعد از پایش آن به مدت زمان DIFS و یا در آغاز هر برش	آنی	T_{idel1}, Ti_{dlel2}
$1-\alpha$ (از مدل برهم‌کنش گره‌ها استخراج می‌شود)	گذار آنی معرف احتمال مشغول بودن کانال بعد از پایش آن به مدت زمان DIFS و یا در آغاز هر برش	//	T_{busy1}, T_{busy2}
τ_{slot}	گذار معرف زمان سپری‌شده برای هر برش	زمان‌دار	T_{slot}
$T_{CTS} + T_{DATA} + T_{ACK}$	گذار معرف زمان تایمر NAV	//	T_{NAV1}, T_{NAV2}
$\frac{phH}{B1} + \frac{RTS}{B2}$	گذار معرف زمان ارسال بسته کنترلی RTS	//	T_{RTS}
$\frac{phH}{B1} + \frac{CTS}{B2} + \tau_{SIFS} + \tau_{CCA} + \tau_{RxTx}$	گذار معرف زمان ارسال بسته کنترلی CTS	//	T_{CTS}
$\frac{phH}{B1} + \frac{MPDU}{B2} + \tau_{SIFS} + \tau_{CCA} + \tau_{RxTx}$	گذار معرف زمان ارسال بسته DATA	//	T_{DATA}
$\frac{phH}{B1} + \frac{ACK}{B2} + \tau_{SIFS} + \tau_{CCA} + \tau_{RxTx}$	گذار معرف زمان ارسال بسته کنترلی ACK	//	T_{ACK}
β(از مدل برهم‌کنش گره‌ها استخراج می‌شود)	گذار معرف احتمال موفقیت‌آمیز بودن مکانیزم دست‌تکانی RTS/CTS	آنی	T_{SUCC}
$1-\beta$ (از مدل برهم‌کنش گره‌ها استخراج می‌شود)	گذار معرف احتمال عدم موفقیت در مکانیزم دست‌تکانی RTS/CTS	آنی	T_{fail}
$2.SIFS + T_{DATA} + T_{ACK}$	گذار معرف زمانی که یک گره صبر می‌کند جهت اجرای یک RTS/CTS جدید	زمان‌دار	$T_{timeout}$
---	گذار آنی که وظیفه آن بازگشت دادن بافر مورداستفاده به فضای بافر گره بعد از MRL تعداد ارسال ناموفق داده در کانال می‌باشد.	آنی	$T_{Buff\text{-}back}$

رابطه کلی زمان این گذارها به‌صورت رابطه ۴-۵ خواهد بود. که در اینجا X می‌تواند طول هریک از بسته‌های CTS، DATA و یا ACK باشد.

$$T = \frac{phH}{B1} + \frac{X}{B2} + \tau_{SIFS} + \tau_{CCA} + \tau_{RxTx} \qquad (۵-۴)$$

با فعال شدن گذار T_{ACK} نیز تمام نشانه‌های مکان‌های P_{RC} و P_{MRL} خالی خواهد شد و یک نشانه به مکان P_{Buff} اضافه شده تا شرایط برای ارسال یک داده جدید برای گره دیگر فراهم باشد. در جدول ۴-۱ زمان فعالیت مرتبط با کلیه گذارهای زمان‌دار و احتمال فعالیت گذارهای آنی ساختار انتخاب که در شکل ۴-۱ از آن‌ها استفاده می‌شود لیست شده است.

از مدل ارائه شده در این بخش می‌توان برای نشان دادن عملیات جزئی اتفاق افتاده در یک گره مشروع و یا یک گره متخاصم استفاده کرد. در مورد گره‌های متخاصم این کار با تغییر پارامترهای عمده آن انجام خواهد شد که شرح جزئیات آن در بخش ۴-۱-۶ مطرح خواهد شد.

۴-۱-۲-مدل برهم‌کنش گره‌ها

همان‌طور که در بخش ۴-۱ مطرح شد علاوه بر مدل جزئی گره‌ها که توصیف‌کننده عملیات پایه هر گره در پیاده‌سازی پروتکل IEEE 802.11 DCF می‌باشد، به مدل دیگری که برهم‌کنش و رقابت بین گره‌ها در ارسال داده در کانال مشترک را نشان می‌دهد، نیاز داریم. مدل موردنظر که در اینجا **مدل برهم‌کنش گره‌ها** نامیده می‌شود در شکل ۴-۲ نشان داده شده است. همان‌طور که در این شکل نشان داده مدل برهم‌کنش گره‌ها از دو جریان ارسال مجزا برای ارسال داده برای گره‌های مشروع[1] و

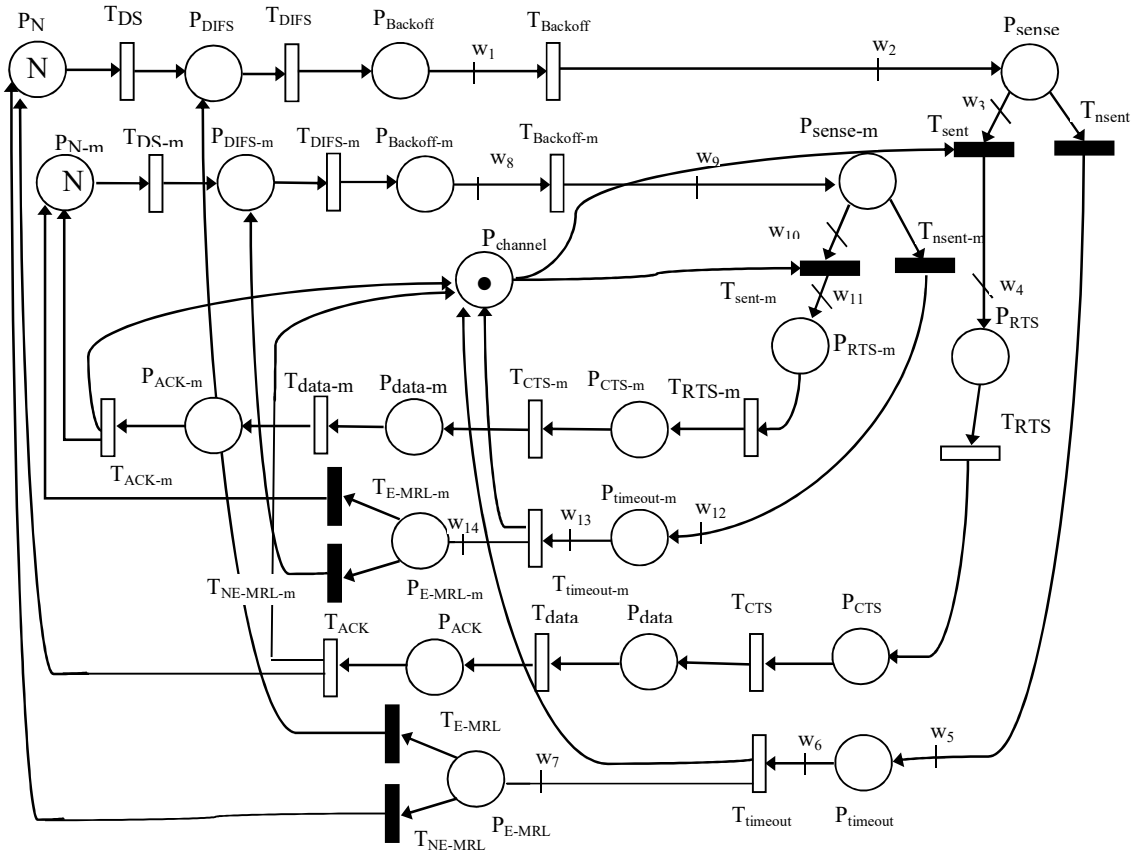
[1] legitimate

گره‌های متخاصم[1] تشکیل شده است. مجموعه گره‌های مورد نظر این مدل شامل گره‌هایی است که در یک همسایگی قرار دارند و از یک کانال مشترک جهت ارسال داده استفاده می‌کنند.

همان‌طور که در شکل ۴-۲ نشان داده شده دو جریان در نظر گرفته شده برای گره‌های مشروع و متخاصم به ترتیب با مکان‌های P_N و P_{N-m} شروع می‌شوند. تعداد نشانه‌های اولیه موجود در این مکان‌ها (N و N_m) به ترتیب نشان‌دهنده تعداد گره‌های مشروع و متخاصم در یک فضای همسایگی می‌باشد که قصد ارسال بسته داده در کانال مشترک را دارند. در بخش ۴-۱-۴ روابط لازم جهت محاسبه N و N_m با فرض پیروی گره‌ها از مدل حرکتی random way point ارائه خواهد شد. فرض می‌شود که هر گره با نرخ ارسال λ، بسته‌های داده را در فضای کانال ارسال می‌کند. این نرخ درواقع برابر توان گذردهی لایه شبکه می‌باشد که مدل آن در بخش ۴-۳ معرفی خواهد شد. با فعال شدن گذار T_{DS} هر گره به اندازه بازه زمانی DIFS کانال را پایش می‌کند و سپس ارسال بسته RTS را به اندازه پنجره انتظار تعویق ، به تأخیر می‌اندازد. این دو زمان انتظار به ترتیب توسط گذارهای T_{DIFS} و $T_{Backoff}$ در مدل برهم‌کنش گره‌ها نشان داده شده‌اند. همانند مدل جزئی هر گره که در شکل ۴-۱ ارائه شده است، زمان لازم جهت اجرای گذار T_{DIFS} از استاندارد موجود در پروتکل IEEE 802.11 DCF استخراج می‌شود. زمان لازم جهت اجرای گذار $T_{Backoff}$ نیز برابر $A_S.T_S$ می‌باشد که در آن A_S برابر متوسط طول پنجره انتظار تعویق می‌باشد. این مقدار معادل متوسط تعداد گره‌های موجود در مرحله انتظار تعویق می‌باشد که با استفاده از رابطه $m(P_{Slot})$ از مدل جزئی گره‌ها در شکل ۴-۱ استخراج می‌شود و زمان کلی آن نیز به شرح رابطه ۴-۶ می‌باشد

$$Time(T_{Backoff}) = A_S.T_s = m(P_{slot}).T_s \qquad (۶-۴)$$

[1] misbehavior



شکل ۴-۲ مدل SRN برهم‌کنش گره‌ها در لایه پیوند داده

طول هر برش زمانی (T_S) نیز از استاندارد موجود در پروتکل IEEE 802.11 DCF به دست می‌آید. با فعال شدن گذار $T_{Backoff}$ کلیه نشانه‌های موجود در مکان $P_{Backoff}$ از آن حذف می‌شوند و درمکان P_{sense} قرار می‌گیرند. به همین منظور وزن کمان‌های w1 و w2 برابر تعداد نشانه‌های موجود در مکان $P_{Backoff}$ می‌باشد. ازآنجاکه در مکان P_{sense} احتمال برخورد بین گره‌ها در ارسال داده بررسی می‌شود، لذا یک ساختار انتخاب[1] د.گانه به‌عنوان خروجی این مکان در نظر گرفته می‌شود. دو خروجی موردنظر توسط گذارهای آنی T_{sent} و T_{nsent} در مدل نشان داده شده اند. T_{sent} برای توصیف حالتی در نظر گرفته

[1] Choice

شده است که گره، داده را با موفقیت در کانال ارسال می‌کند و T_{nsent} نیز برای حالتی است که گره در فرآیند ارسال داده دچار برخورد می‌شود. رابطه احتمال مرتبط با فعال شدن این دو گذار آنی (μ برای T_{nsent} و μ-۱ برای T_{sent}) در بخش ۴-۱-۳ محاسبه خواهد شد که ارتباط مستقیمی با تعداد گره‌های مشروع و متخاصم موجود در یک همسایگی که قصد ارسال داده را دارند، دارد.

در صورت عدم ایجاد برخورد در ارسال داده توسط گره‌های موجود در یک همسایگی، گذار T_{nsent} فعال شده و عملیات پایه RTS/CTS را مطابق با آنچه در بخش مدل جزئی گره‌ها بیان شده با استفاده از گذارها و مکان‌هایP_{RTS} ،T_{RTS}، P_{CTS}،T_{CTS}، T_{ACK} ,P_{DATA} ,P_{ACK} و T_{DATA} ، انجام می‌شود. وزن کمان w_3 تضمین می‌کند که تمام گره‌های که در حال رقابت برای ارسال داده بودند و عملیات انتظار تعویق را به‌درستی انجام داده‌اند بتوانند عملیات پایه RTS/CTS را آغاز کنند. هر گره برای ارسال داده نیازمند آزاد دیدن کانال است که این مورد در صورت حضور نشانه در مکان $P_{channel}$ محقق خواهد شد. با اتمام مراحل RTS/CTS نیز کانال آزاد شده که این مورد با برگشت دادن نشانه به مکان $P_{channel}$ نشان داده شده و همچنین یک گره به مجموع گره‌هایی که در صف ارسال داده هستند اضافه می‌شود. مورد آخر توسط کمان اتصالی از گذار TACK به مکان P_N در مدل نشان داده شده است.

در صورت فعال شدن گذار T_{nsent} یک پیغام timeout ارسال خواهد شد که این مورد توسط گذار $T_{timeout}$ نشان داده شده است. در این صورت (ناموفق بودن ارسال داده توسط یک گره و ارسال پیغام timeout) تمام گره‌ها ارسال داده خود را در کانال لغو خواهند کرد. به همین منظور وزن کمان‌های w4، w5 و w6 برابر تعداد نشانه‌های موجود در مکان P_{sense} می‌باشد. مجموعه گره‌هایی که دچار برخورد شده‌اند درصورتی‌که تعداد تلاش انجام شده برای آن‌ها در ارسال داده برابر حداکثر تلاش اجازه

داده شده برای ارسال داده MRL[1] باشد در آن صورت بسته داده از بین رفته و گره مجدداً در صف ارسال داده قرار می‌گیرد. در غیر این صورت گره اجازه خواهد داشت تا مجدداً کانال را به اندازه بازه زمانی DIFS پایش کرده و عملیات ارسال داده را انجام دهد. احتمال مرتبط با هریک از این دو پیشامد توسط ساختار انتخاب و گذارهای آنی $T_{E\text{-}MRL}$ (گره به حداکثر تعداد تلاش برای ارسال داده در کانال رسیده است) و$T_{NE\text{-}MRL}$ (گره به حداکثر تعداد تلاش برای ارسال داده در کانال نرسیده است) نشان داده شده است. رابطه احتمال مرتبط با هریک از این دو پیشامد (δ برای $T_{E\text{-}MRL}$ و (δ-۱) برای $T_{NE\text{-}MRL}$) در بخش ۴-۱-۳ محاسبه خواهد شد.

مکانیزم ارائه شده در رقابت گره‌های مشروع برای تصاحب کانال جهت ارسال داده برای گره‌های متخاصم نیز به همین صورت می‌باشد با این تفاوت که این گره‌ها از پارامترهای با مقادیر متفاوتی استفاده می‌کنند که شانس این گره‌ها را برای تصاحب کانال افزایش می‌دهد. به همین منظور جریان جداگانه‌ای برای توصیف عملکرد آن‌ها در مدل ارائه شده است که با یک پسوند m– با مکان و یا گذار متناظر با آن در جریان موجود برای گره‌های مشروع متمایز شده است. مطابق با توضیحات ارائه شده در بخش ۲-۱-۳-۲ تغییرات ممکنه برای اعمال هریک از حملات لایه پیوند داده ارائه خواهد شد. با وجود دقت در طراحی مدل SRN ارائه شده جهت انطباق آن با پروتکل IEEE 802.11 DCF برای اطمینان بیشتر از صحت آن می‌توان از توابع نگهبان[2] که در بخش ۳-۴ راجع به آن توضیح داده شد استفاده کرد. این توابع با اعمال روی گذارهای مدل سبب جلوگیری از فعال شدن آن در موارد اشتباه ناخواسته که با اصول پروتکل IEEE 802.11DCF مطابقت ندارد، می‌شود.

[1] Maximum Retry Limit
[2] Guard function

جدول ۴-۲ توابع نگهبان مورداستفاده در مدل SRN شکل ۴-۲

شماره تابع	نام گذار	تابع نگهبان
۱	$T_{DIFS,}$ T_{DIFS-m}	(m(P_{RTS})+m(P_{CTS})+m(P_{data})+m(P_{ACK})+m(P_{sense})+m($P_{timeout}$)+m(P_{RTS-m}) +m(P_{CTS-m})+m(P_{data-m})+m(P_{ACK-m})+m($P_{sense-m}$)+m($P_{timeout-m}$)=0 and m(P_{ch}=1)
۲	$T_{backoff,}$ $T_{backoff-m}$	(m(P_{RTS})+m(P_{CTS})+m(P_{data})+m(P_{ACK})+m(P_{sense})+m($P_{timeout}$)+m(P_{RTS-m})+ m(P_{CTS-m})+m(P_{data-m})+m(P_{ACK-m})+m($P_{sense-m}$)+m($P_{timeout-m}$)=0 and m(P_{ch}=1)
۳	T_{sent}, T_{sent-m}	(m(P_{CTS})+m(P_{data})+m(P_{ACK})+m($P_{timeout}$)+m(P_{CTS-m})+m(P_{data-m})+m(P_{ACK-m})+(m($P_{timeout-m}$)=0) and (m(P_{ch})=1)

جدول ۴-۳ توابع نگهبان مورداستفاده در مدل SRN شکل ۴-۲

Weight	***Arc name***
w_1, w_2	$m(P_{Backoff})$
w_3, w_4, w_5	$m(P_{sense})$
w_7, w_6	$m(P_{timeout})$
w_8, w_9	$m(P_{Backoff-m})$
w_{10}, $w_{11,}$ w_{12}	$m(P_{sense-m})$
w_{13}, w_{14}	$m(P_{timeout-m})$

در جدول ۴-۲ تمام توابع نگهبان مورداستفاده در مدل برهم‌کنش گره‌ها ارائه شده است. همچنین وزن کمان‌های به کار رفته در مدل برهم‌کنش گره‌ها در جدول ۴-۳ ارائه شده است.

۴-۱-۳-استخراج پارامترهای مرتبط با مدل

در هریک از دو مدل ارائه شده برای بررسی رفتار گره‌ها در لایه انتقال داده پارامترهایی وجود دارد که مقدارشان از خود مدل به دست می‌آید. این پارامترها مرتبط با زمان فعالیت یک گذار زمان‌دار و یا احتمال فعال شدن یک گذار آنی هستند. در مدل جزئی گره‌ها دو ساختار انتخاب (T_{busy1} - T_{idle1}) و (T_{busy1} - T_{idle1}) به دلیل یکسان بودن مقدار احتمالشان، هرکدام با α مدل شده‌اند. احتمال مرتبط با گذارهای ساختار انتخاب (T_{busy1} - T_{idle1}) نیز با β مدل شده است. α درواقع نشان‌دهنده احتمال

مشغول بودن کانال می‌باشد. برای استخراج این پارامتر از مدل در نگاه اول شاید به نظر برسد که مقدار احتمال مرتبط با آن برابر احتمال عدم وجود نشانه در مکان P_{ch} برابر $Pr(P_{ch}=0)$ باشد. اما مواردی که گره‌ای در حال ارسال داده و یا انجام مراحل پروتکل دست تکانی RTS/CTS می‌باشد هم باید در رابطه احتمالاتی موردنظر گنجانده شود.

$$\alpha = Pr(T_{bus}\ ) = Pr(T_{bus}\ ) = Pr(\neq P_{ch}=0\ or\ \neq P_{CTS}>0\ or\ \neq P_{data}>0\ or\ \neq P_{ACK}>0\ or\ \neq P_{CTS-m}>0\ or\ \neq P_{data-}\ >0\ or\ \neq P_{ACK-m}>0) \quad (۶\text{-}۴)$$

$$Pr(T_{idle1}) = Pr(T_{idle}\ ) = 1-\alpha \quad (۷\text{-}۴)$$

همچنین، β که نشان‌دهنده احتمال شکست در ارسال داده از طریق کانال توسط یک گره می‌باشد ($Pr(T_{fail})$) با استفاده از رابطه ۴-۸ به دست می‌آید. $P\,r(T_{succ})$ نیز بر اساس رابطه ۴-۹ محاسبه می‌شود.

$$\beta = Pr(T_{fail}) = \frac{Thr(T_{n-sen}\ )}{Thr(T_{n-sen}\ )+Thr(T_{sent})} \quad (۸\text{-}۴)$$

$$P\,r(T_{succ}) = 1-\beta \quad (۹\text{-}۴)$$

در مدل برهم‌کنش گره‌ها دو پارامتر هستند که از دل مدل جزئی گره‌ها به دست می‌آید. μ به‌عنوان اولین پارامتر، نشان‌دهنده احتمال آن است که یک گره نتواند داده را با موفقیت در کانال ارسال کند. بر اساس کار انجام شده در [۳۸] دو اتفاق ممکن است سبب شکست در ارسال داده توسط یک گره با وجود تبعیت از مکانیزم RTS/CTS شود.

اتفاق ۱: دو گره به‌صورت هم‌زمان شروع به پایش کانال نمایند که در آن صورت بازه انتظار DIFS را باهم به اتمام می‌رسانند و برحسب اتفاق تعداد پنجره انتظار تعویق یکسانی نیز کسب نمایند. احتمال این رخداد ارتباط مستقیمی با تعداد گره‌های موجود در یک همسایگی و ارتباط معکوسی با تعداد برش‌های زمانی پنجره انتظار تعویق دارد. متوسط تعداد برش‌های زمانی که یک گره در پنجره انتظار

تعویق خود طی می‌کند برابر A_S می‌باشد که بر اساس آنچه در بخش قبل مطرح شد، A_S برابر $m(P_{slot})$ است. از طرفی تعداد گره‌هایی که در یک همسایگی قرار دارند و به‌طور هم‌زمان در حال گذراندن پنجره انتظار رقابت خود هستند برای گره‌های مشروع و متخاصم به ترتیب برابر $m(P_{Backoff})$ و $m(P_{Backoff-m})$ می‌باشد. با این توضیحات، احتمال رخداد اتفاق ۱ ($prob_1$) بر اساس رابطه احتمالاتی معادله ۴-۱۰ به دست می‌آید.

$$prob_1 = 1 - ((1 - \frac{1}{A_S})^{m(P_{Backoff})} \times (1 - \frac{1}{A_{S-m}})^{m(P_{Backoff-m})}) \qquad (۱۰-۴)$$

اتفاق ۲: یک گره که در ناحیه مخفی گره فرستنده A قرار دارد، اقدام به ارسال داده‌ای می‌کند که خارج از ناحیه تداخل گره گیرنده B قرار دارد که ممکن است با دریافت داده توسط گره گیرنده B تداخل ایجاد کند. به‌طور متوسط مدت زمانی که این مشکل ممکن است رخ دهد در بازه انتقال داده توسط یک گره می‌باشد. با توجه به آنکه انتقال داده نیز در بازه‌های زمانی τ_{slot} انجام می‌شود لذا تعداد بازه‌های زمانی ممکنه برای رخداد این اتفاق برابر $\frac{T_{data}}{T_{slot}}$ می‌باشد که برای هریک از گره‌های واقع در ناحیه مخفی گره B (N_h) احتمال رخداد آن وجود دارد. رابطه محاسبه N_h در بخش ۴-۱-۵ ارائه خواهد شد و بر اساس آن رابطه احتمال مربوط به اتفاق ۲ ($prob_2$) مطابق با معادله ۴-۱۱ می‌باشد.

$$prob_2 = 1 - (1 - \frac{T_{data}}{T_{slot}})^{N_h} \qquad (۱۱-۴)$$

لذا احتمال کلی مرتبط با رخداد T_{nsent}، μ برابر معادله ۴-۱۲ خواهد بود.

$$\mu = pr(T_{nsent}) = 1 - ((1 - prob_1)(1 - prob_2)) \qquad (۱۲-۴)$$

$$pr(T_{sent}) = 1 - \mu \qquad (۱۳-۴)$$

احتمال رخداد مرتبط با ساختار انتخاب ($T_{E\text{-}MRL} - T_{NE\text{-}MRL}$) نیز که از مدل جزئی گره‌ها به دست می‌آید معرف احتمال رخدادی است گره به حداکثر تلاش مجاز جهت ارسال داده (MRL) رسیده و

هنوز موفق به ارسال آن نشده است. احتمال این رخداد توسط δ نشان داده شده و توسط رابطه ۴-۱۴ توصیف شده است.

$$Pr(T_{E-MRL}) = \delta = Pr(m(P_{MRL}) = 0 \; and \; m(P_{Buff-back}) > 0\,) \qquad (۱۴-۴)$$

$$Pr(T_{NE-M}\;\;) = 1 - \delta \qquad (۱۵-۴)$$

۴-۱-۴-روابط لازم جهت محاسبه تعداد گره در یک فضای همسایگی

همان‌طور که در بخش ۴-۱-۳ بیان شد برای حل مدل برهم‌کنش گره‌ها نیاز به محاسبه متوسط تعداد گره‌های موجود در یک فضای همسایگی خواهیم داشت. در مدل برهم‌کنش گره‌ها از این مقدار به‌عنوان تعداد نشانه اولیه در مکان P_N و نسبت تعداد گره‌های متخاصم برای مکان $P_{N\text{-}m}$ استفاده خواهد شد. در این بخش روابط ریاضی لازم جهت محاسبه تعداد گره‌های موجود در یک فضای همسایگی (N) را با فرض وجود M گره در شبکه‌ای با مساحت A و اندازه بعد a ارائه خواهیم کرد. در محاسبات پیش رو فرض می‌شود که گره‌ها از مدل حرکتی RWP[1] پیروی می‌کنند. بر اساس این مدل حرکتی، هر گره مقصد دلخواهی را در شبکه انتخاب می‌کند و با سرعتی که بین دو مقدار V_{min} و V_{max} به‌صورت یکنواخت انتخاب می‌شود حرکت می‌کند. بعد از رسیدن گره به مقصد، در آنجا به اندازه زمان مکث[2] توقف دارد و سپس با رویکرد مشابه‌ای به سمت مقصد جدید حرکت می‌کند. بر اساس مطالعات انجام شده در [۶۳] با وجودآنکه موقعیت گره‌ها در ابتدا از یک توزیع نرمال استفاده می‌کند، در اجراهای طولانی‌مدت، توزیع فضای حرکتی گره‌ها رویکردی غیریکنواخت پیدا خواهد کرد. همچنین در اجراهای طولانی، برای یک گره، احتمال حضور آن در مرکز ناحیه حرکت گره‌ها دارای

[1] Random Way Point
[2] Pause time

مقدار زیاد و احتمال حضور آن در اطراف ناحیه حرکت گره‌ها نزدیک به صفر خواهد بود. لذا تابع توزیع احتمال جایگشت گره‌ها تحت توپولوژی RWP به‌صورت فرمول ۴-۱۶ محاسبه می‌شود.

$$f_x(x, t > 0) = P_p f_{x,p}(x) + (1 - P_p) f_{x,m}(x) \qquad (۱۶\text{-}۴)$$

که در آن $f_{x,m}(x)$ تابع توزیع احتمال جایگشت گره‌های متحرک $f_{x,p}(x)$ نیز تابع توزیع احتمال جایگشت گره‌های ساکن می‌باشد. P_p متناظر با احتمال توقف گره در بازه مکث می‌باشد که بر اساس رابطه ۴-۱۷ محاسبه خواهد شد. در این رابطه τ_P مدت زمان مکث می‌باشد و $E(T)$ نیز مدت زمان سپری‌شده جهت گذر گره بین دو نقطه ثابت می‌باشد که توسط رابطه ۴-۱۸ نشان داده شده است.

$$P_p = \frac{\tau_P}{\tau_P + E(T)} \qquad (۱۷\text{-}۴)$$

$$E(T) = \frac{0.9054a}{V_{max} - V_{min}} \ln\left(\frac{V_{max}}{V_{min}}\right) \qquad (۱۸\text{-}۴)$$

با جایگذاری این رابطه در تابع توزیع احتمال درجه هر گره، رابطه توزیع احتمال تعداد گره‌های موجود در ناحیه همسایگی گره‌ای که در موقعیت x قرار دارد، بر اساس رابطه ۴-۱۹ خواهد بود.$N_{0,p}$ در این رابطه متناظر با تعداد گره‌های ساکن و$N_{0,m}$ نیز نشان‌دهنده تعداد گره‌های در حال حرکت و موجود در فضای همسایگی گره موجود در موقعیت x خواهد بود.

$$N_0(x) = P_p N_{0,p}(x) + (1 - P_p) N_{0,m}(x) \qquad (۱۹\text{-}۴)$$

که بر اساس مطالعات صورت گرفته در همین مراجع مقدار$N_{0,p}$ و$N_{0,m}$ به ترتیب از رابطه‌های ۴-۲۰ و ۴-۲۱ به دست می‌آید.

$$N_{0,p} = M \times {r_a}^2 \left(1 - \frac{4}{3\pi} \times r_a\right) \qquad (۲۰\text{-}۴)$$

$$N_{0,m} = \frac{M}{4\pi}\Big[4.{r_a}^2(2.r^2 + {r_a}^2 - 2).arcsin\left(\frac{r^2 + {r_a}^2 - 1}{2.r.r_a}\right) - 4arcsin\left(\frac{r^2 + {r_a}^2 - 1}{2.r.r_a}\right) + \sqrt{\omega}(r^2 + 5{r_a}^2 - 3) + 2\pi(-2r^2{r_a}^2 + 2.r^2 - {r_a}^4 + 1)\Big] \qquad (۲۱\text{-}۴)$$

که در آن $\omega = (r + r_a + 1)(-r + r_a + 1)(r - r_a + 1)(r + r_a 11)$ می‌باشد. در رابطه‌های بالا r_a متناظر با شعاع انتقال گره و r نیز برابر فاصله گره تا مرکز ناحیه A می‌باشد که با انتگرال‌گیری روی r مقدار نهایی N ، برابر رابطه ۴-۲۲ خواهد بود.

$$N = N_{r_a}^{RWP} = \frac{r_a^2}{3}\left(\left(4 - 2P_p + {P_p}^2\right) - \frac{4}{\pi}{P_p}^2 r_a - 3\left(1 - P_p\right){r_a}^2\right) \times M \qquad (۲۲-۴)$$

در به دست آوردن N_m که نشان‌دهنده تعداد گره‌های متخاصم موجود در یک همسایگی هست نیز کافی است به‌جای M از M_m که نشان‌دهنده تعداد کل گره‌های متخاصم موجود در شبکه است استفاده کنیم.

۴-۱-۵-روابط لازم جهت محاسبه تعداد گره در ناحیه مخفی

همان‌طور که در بخش ۴-۱-۳ گفته شد در محاسبات مربوط به مدل برهم‌کنش گره‌ها و در محاسبه احتمال ارسال موفقیت‌آمیز داده توسط یک گره در کانال مشترک موجود در یک همسایگی، نیازمند محاسبه تعداد گره موجود در ناحیه مخفی هستیم. تعداد گره‌های موجود در این ناحیه تزاحم مستقیمی بر افزایش احتمال برخورد در ارسال داده خواهد داشت. بر اساس مطالب گفته‌شده در بخش ۳-۱-۲ مساحت ناحیه مخفی که وابسته به شعاع تداخل[1]، فاصله بین فرستنده و گیرنده و قدرت سیگنال ارسالی بین آن‌ها می‌باشد. معمولاً در فضای تبادل اطلاعات بین گره‌های گیرنده و فرستنده اصلی، اطلاعات ارسالی بین گره‌های دیگر می‌تواند به‌صورت اختلال[2] در آن تأثیر منفی داشته باشد. اصولاً برای دریافت مناسب سیگنال توسط گره گیرنده لازم است تا نرخ سیگنال به نویز[3] از یک حد خاص بیشتر باشد که اصولاً به آن TSNR[4] اطلاق می‌شود. درصورتی‌که P_r، قدرت سیگنال ارسال از طرف گره اصلی که در فاصله d متر از گره گیرنده قرار دارد و P_i نیز قدرت سیگنال ارسالی (نویز) از

[1] Interference range
[2] Noise
[3] Signal to Noise Ratio (SNR)
[4] Threshould of Signal to Noise Ration (TSNR)

طرف گره دیگر در محدوده گره گیرنده باشد که در فاصله r از آن قرار دارد بنابراین $SNR = {P_r}/{P_i}$. با فرض این‌که تمام گره‌های رادیویی همگن[1] و در یک محیط فضای باز[2] باشند، P_r از رابطه ۴-۲۳ محاسبه خواهد شد [۲۹،۳۰]. در این رابطه G_t و G_r به ترتیب معرف نرخ بهره[3] آنتن فرستنده و گیرنده می‌باشد. ht و hr نیز نشان‌دهنده ارتفاع آنتن‌های فرستنده و گیرنده می‌باشند. TSNR نیز بر اساس رابطه ۴-۲۴ محاسبه خواهد شد.

$$P_r = P_t G_t G_r \frac{h_t^2 h_r^2}{d^k} \qquad (۲۳-۴)$$

$$SNR = {P_r}/{P_i} = \frac{P_t G_t G_r \frac{h_t^2 h_r^2}{d^k}}{P_t G_t G_r \frac{h_t^2 h_r^2}{r^k}} = \left(\frac{r}{d}\right)^k \geq T_{SNR} \qquad (۲۴-۴)$$

آنچه از این رابطه تفسیر می‌شود آن است که برای دریافت صحیح سیگنال از گره فرستنده لازم است تا فاصله آن از گره متداخل[4] که نویز آن روی دریافت سیگنال توسط گره گیرنده تأثیر می‌گذارد حداقل به اندازه $r \geq \sqrt[k]{T_{SNR}} * d$ باشد. لذا شعاع محدوده رادیویی کمتر از این مقدار به‌عنوان شعاع ناحیه تداخل (R_i) شناخته می‌شود.

$$R_i = \sqrt[k]{T_{SNR}} * d \qquad (۲۵-۴)$$

بر اساس [۲۹] مقدار T_{SNR} برابر ۱۰ در نظر گرفته می‌شود. همچنین در شبکه با گره‌های متجانس نیز مقدار k را برابر ۴ در نظر می‌گیرند. بنابراین به‌منظور تعیین مقدار دقیق R_i کافی است تا رابطه فاصله متوسط بین گره فرستنده و گیرنده متوالی در یک شبکه محاسبه شود. بر اساس مطالعه صورت گرفته

[1] Homogeneous
[2] open space environment
[3] antenna gain
[4] Interfering node

در [۶۴] نشان داده شده است که متوسط فاصله دو گره متوالی (d) در یک مسیر که دارای شعاع انتقال R_t می‌باشند برابر رابطه ۴-۲۶ می‌باشد.

$$f_r(d) = \frac{2N_r}{2N_r+1}.Rt \qquad (۲۶-۴)$$

که با جایگذاری آن در رابطه ۴-۲۵ مقدار متوسط شعاع ناحیه تداخل برابر رابطه ۴-۲۷ خواهد بود.

$$R_i = \frac{2N_r}{2N_r+1}.\sqrt[k]{T_{SNR}}\,.Rt \qquad (۲۷-۴)$$

به‌منظور استخراج دقیق مساحت ناحیه مخفی لازم است مساحت فضای مشترک بین ناحیه گوش دادن گره فرستنده و ناحیه تداخل گره گیرنده را از ناحیه تداخل گیرنده کم کنیم. بر اساس مطالعات هندسی صورت گرفته در [۶۴] مساحت ناحیه مشترک بین دو دایره با شعاع R_1 و R_2 به‌صورت رابطه کلی ۴-۲۸ خواهد بود.

$$A_{int}(R_1,R_2,d_x) = P1(R_1,R_2,d_x) + P2(R_1,R_2,d_x) + P3(R_1,R_2,d_x) \qquad (۲۸-۴)$$

که در آن d_x ناظر به فاصله میان شعاع دو دایره می‌باشد و $P1$، $P2$ و $P3$ با استفاده از روابط زیر به دست می‌آیند.

$$P1(R_1,R_2,d_x) = {R_1}^2.Arccos(\frac{{d_x}^2 + {R_1}^2 - {R_2}^2}{2d_x.R_1})$$

$$P2(R_1,R_2,d_x) = {R_2}^2.Arccos(\frac{{d_x}^2 + {R_2}^2 - {R_1}^2}{2d_x.R_1})$$

$$P3(R_1,R_2,d_x) = \frac{1}{2}\sqrt{(-d_x+R_1+R_2).(d_x+R_1-R_2).(d_x+R_1+R_2)}$$

بنابراین مساحت ناحیه مخفی برای گره گیرند x که شعاع ناحیه تداخل آن R_i و دارای فاصله d_x از گره فرستنده با شعاع ناحیه گوش دادن R_{cs} می‌باشد، بر اساس رابطه ۴-۲۹ محاسبه خواهد شد.

$$A_h(x) = \pi.(R_i(x))^2 - A_{int}(R_{cs},R_i,d_x) \qquad (۲۹-۴)$$

با توجه به اینکه ناحیه مخفی بخشی از ناحیه تداخل می‌باشد، می‌توان با محاسبه تعداد کل گره‌های موجود در ناحیه تداخل، به نسبت سهم ناحیه مخفی از آن، تعداد گره‌های موجود در ناحیه مخفی (N_h) را حساب کرد. لذا رابطه نهاییN_h بر اساس رابطه ۴-۳۰ خواهد بود.؛ که در آنN_i نشان‌دهنده تعداد گره‌های موجود در ناحیه تداخل می‌باشد که با جایگذاری R_i در رابطه ۴-۲۲ به دست می‌آید.

$$N_h = \frac{A_h}{A_h + A_{int}} \times N_i \qquad (۳۰-۴)$$

۴-۱-۶-پیاده‌سازی مدل اعمال حملات

در ذیل تغییرات لازم جهت پیاده‌سازی و اعمال حملات لایه پیوند داده در مدل SRN ارائه شده جهت این لایه را بررسی می‌کنیم. تعریف دقیق چگونگی هریک از این حملات در بخش ۲-۱-۳-۲ ارائه شده است.

حمله دست‌کاری پنجره انتظار تعویق: در این نوع حمله همان‌طور که مطرح شد گره متخاصم این استراتژی را استفاده می‌کند که با هر بار شکست در ارسال داده در کانال، طول پنجره انتظار تعویق را افزایش نمی‌دهد. از این طریق گره متخاصم دارای شانس بیشتری در تصاحب کانال در مقایسه با گره‌های مشروعی می‌باشد که طول پنجره انتظار تعویق آن‌ها از قانون عادی برای افزایش استفاده می‌کند. برای اعمال این حمله ابتدا مقدار RNS (وزن کمان بین T_{idle1} به سمت P_{sense2}) در مدل ارائه شده برای رفتار جزئی گره‌ها در شکل ۴-۱ به‌جای رابطه ۲-۱ از رابطه ۴-۳۱ به دست می‌آید که در آن مقدار RC همیشه برابر یک خواهد بود. بر اساس این مقدار زمان اجرای گذار$T_{Backoff}$ نیز به‌صورت رابطه ۴-۳۲ خواهد بود.

$$RNS' = (CW_{min} + 1).2^{RC} - 1 \mid Rc = 1 \qquad (۳۱-۴)$$

$$Time(\ _{Backoff}) = A_s.T_s = m(P_{slot}).T_s \mid E(T_{idle1}, P_{s-slo}\ ) = RNS' \qquad (۳۲-۴)$$

همچنین مقادیر δ و μ برای جریان موجود برای گره‌های متخاصم در مدل برهم‌کنش گره‌ها با تغییرات اعمال‌شده در مدل جزئی گره‌ها از آن استخراج شده و به گذارهای مرتبط با آن اعمال می‌شود.

حمله دست‌کاری بازه انتظار DIFS: در این نوع از حمله، گره متخاصم بازه انتظار DIFS را به مقدار کوچک‌تری (معمولاً نصف آن) تنظیم می‌کند. به همین منظور زمان اجرای گذار T_{DIFS} از رابطه زیر به دست می‌آید. همچنین مقادیر δ و μ برای جریان موجود برای گره‌های متخاصم در مدل برهم‌کنش گره‌ها با تغییرات اعمال‌شده در مدل جزئی گره‌ها از آن استخراج شده و به گذارهای مرتبط با آن اعمال می‌شوند.

$$Time(T_{DIFS}\quad) = \frac{\tau_{DIFS}}{2} \qquad (۳۳-۴)$$

حمله دست‌کاری تایمر NAV: در این نوع از حمله، گره متخاصم با شنیدن پیغام‌های RTS تایمر NAV خود را به‌گونه‌ای تنظیم می‌کند تا بتواند در مرحله بعدی از پروتکل دست تکانی RTS/CTS گره ارسال‌کننده جاری را دچار برخورد کند. بنابراین برای گره متخاصم $Time(T_{NAV}) = T_{CTS}$ خواهد شد. این تغییر در مدل جزئی گره اعمال‌شده و پارامترهای مقادیر δ و μ از آن استخراج شده و به گذارهای مرتبط برای جریان موجود برای گره‌های متخاصم در مدل برهم‌کنش گره‌ها اعمال می‌شوند.

حمله دست‌کاری سرعت ارسال داده: در این نوع از حمله گره متخاصم سعی می‌کند با کاهش سرعت ارسال داده خود در کانال گره‌های منتظر دیگر را به اشتباه بیندازد و باعث شود تا آن‌ها در تلاش بعدی‌شان دچار برخورد در ارسال داده خود شوند. گره‌های مشروع که تایمر NAV خود را مطابق با سرعت استاندارد ارسال داده توسط تنظیم کردند. این درحالی است که گره‌های متخاصم برای ارسال داده خود زمان بیشتری را طلب می‌کنند و این باعث می‌شود تا گره‌های مشروع با احتمالی در تلاش بعدی‌شان دچار برخورد شوند که این امر در نهایت سبب بالا رفتن احتمال رسیدن به حداکثر تلاش مجاز و حذف شدن بسته داده می‌شود. گره‌های بی‌سیم معمولاً از ۲ سرعت متفاوت،

B1 برای ارسال بسته‌های سرآیند و بسته‌های کنترلی و B2 برای بسته‌های داده استفاده می‌کنند. که B2 دارای سرعت بالاتری از B1 است. با تنظیم سرعت جدید و انتصاب آن به T_{DATA} در مدل جزئی گره‌ها و $T_{DATA\text{-}m}$ در مدل مدل برهم‌کنش گره‌ها پارامترهای ارزیابی جدید از مدل استخراج خواهد شد.

$$Time(T_{DATA}) = \frac{phH}{B1} + \frac{MPDU}{B1} + \tau_{SIFS} + \tau_{CCA} + \tau_{RxTx} \qquad (۳۴-۴)$$

۴-۲- توصیف مدل لایه شبکه

هدف اصلی از این بخش، مدل‌سازی و تجزیه‌وتحلیل عملکرد لایه شبکه در شبکه‌های موردی سیار تحت عملکرد گره‌های مهاجم می‌باشد. مدل ارائه شده لازم است تا رفتار نرمال گره‌های مشروع را علاوه بر رفتار ناهنجار گره‌های مهاجم ارائه کند. با انتخاب AODV به‌عنوان پروتکل مسیریابی انتخاب‌شده، دو جریان مجزا در لایه شبکه یک شبکه موردی سیار وجود خواهد داشت.

۱. جریان اولیه که برای پیدا کردن مسیر از گره مبدأ به مقصد نیاز است که به‌عنوان فرآیند مسیریابی شناخته می‌شود. این فرآیند در مواردی که مسیر به دست آمده دچار مشکل شود نیز استفاده خواهد شد. این حالت مسیر ایجاد شده اولیه‌ترمیم شده و یا آنکه مجدداً مسیر جدیدی ایجاد خواهد شد.
۲. جریان داده که بر اساس مسیر تولیدشده توسط فرآیند اولیه مسیریابی، از گره مبدأ به سمت گره مقصد در جریان است.

وجود این دو جریان متفاوت این ایده را به ذهن متبادر می‌کند که از دو مدل جداگانه یکی برای نشان داده جریان داده و یکی هم برای نشان دادن فرآیند مسیریابی استفاده شود. طبعاً مدل اصلی در اینجا مدل جریان داده می‌باشد و از مدل ارائه شده برای فرآیند مسیریابی در دل مدل ارائه شده برای جریان داده استفاده خواهد شد. با توجه به اینکه یک گره مهاجم در لایه شبکه می‌تواند در هریک از

مراحل مسیریابی و یا ارسال جریان داده اختلال ایجاد کند لذا، رفتار یک گره مهاجم لازم است در هر دو مدل بررسی شود. در ادامه، اطلاعات دقیق‌تری از دو مدل ارائه شده به همراه مقادیر مربوط به پارامترهای آن در بخش‌های بعدی ارائه شده است.

۴-۲-۱-مدل SRN برای فرآیند جریان داده‌ها

با توجه به اینکه جریان داده مرتبط با یک گره در یک شبکه بی‌سیم شامل دو جریان داده ورودی به گره و جریان داده خروجی از گره می‌باشد لذا، مدل ارائه شده برای پردازش جریان داده طراحی شده شامل دو بخش می‌باشد: جریان داده ورودی و جریان داده خروجی. جریان داده ورودی ناظر بر جریان داده‌ای است که از طرف گره‌های دیگر ایجاد شده و تنها به‌این‌علت به گره جاری وارد شده است که این گره در مسیر جریان داده موجود برای انتقال داده از گره مبدأ S به گره مقصد D قرار گرفته است. جریان داده خروجی نیز ناظر بر جریان داده‌ای است که از سمت گره جاری ایجاد و ارسال شده است که در یک شبکه واقعی معمولاً با CBR و یا FTP تولید می‌شوند. همچنین مدل ارائه شده رفتار یک گره در شبکه را مدل می‌کند.

همان‌طور که لایه شبکه در شبکه‌های موردی سیار در سطح انتزاع بالاتری نسبت به لایه پیوند داده قرار دارد، در مدل ارائه شده برای لایه شبکه نیز این مورد لحاظ شده است و به فرآیندهای صورت گرفته در آن درسطح انتزاع بالاتری نگریسته شده است. مدل ارائه شده یک ارتباط یک گامه را در انتقال داده در سطح لایه شبکه را نشان می‌دهد. همچنین از مدل ارائه شده برای لایه پیوند داده در بخش قبل برای محاسبه زمان لازم جهت انتقال داده یک‌گامه در بستر کانال مشترک موجود در یک فضای همسایگی استفاده می‌کند. نتایج به دست آمده از این مدل در محاسبات مربوط به یک مسیر کامل در یک ارتباط انتها به انتها برای رسیدن بسته داده از مبدأ S به مقصد D لحاظ خواهد شد.

همان‌طور که در شکل ۴-۳ برای مدل جریان داده مشخص شده است، جریان داده خروجی با گذار T_{out} آغاز می‌شود. نرخ فعال شدن این گذار با نماد λ نشان داده می‌شود که به‌عنوان یک پارامتر شبکه

می‌باشد. این نرخ همان نرخ تولید بسته در یک شبکه است. در یک شبکه واقعی، بسته‌ها معمولاً با CBR و یا FTP تولید می‌شوند که توسط λ قابل تفسیر می‌باشند. بسته تولیدشده برای شروع فرایند مسیریابی به یک فضای بافر نیاز دارد. بسته‌هایی که در گره جاری منتظر تصرف یک بافر هستند با استفاده از مکان P_{WB} نشان داده می‌شوند. وقتی موفق به تصرف بافر شوند بسته داده خود را به جریان خواهند انداخت. در این مدل، اگر حداقل یک نشانه از استاندارد فضای بافر K در لایه شبکه وجود داشته باشد این گذار فعال خواهد شد و نشانه به مکان P_{wr} انتقال پیدا می‌کند تا عملیات مسیریابی در آن انجام شود.

با توجه به مسائل مدل‌سازی، از فرآیند مسیریابی اولیه چشم‌پوشی کرده و فرض می‌شود که مسیر اولیه در ابتدای کار ایجاد شده است. در فواصل زمانی مختلف ممکن است به دلیل حرکات گره‌ها و یا مسائل دیگر این مسیر دچار شکست شود که در این حالت لازم است مسیر مجدداً ایجاد شود. گذار مرتبط با خرابی مسیر با T_{fail} نشان داده شده است که نرخ فعال شدن مرتبط با این گذار از نتایج مطالعه صورت گرفته در [۶۱ و ۵۹] محاسبه شده است. نویسندگان این تحقیق اقدام به ارائه یک مدل شبکه پتری به‌منظور مطالعه قابلیت دسترسی مسیر[1] در یک شبکه موردی سیار نمودند. در مدل ارائه شده با کمک روابط ریاضی، تأثیر پارامترهایی چون محدوده انتقال گره، ابعاد شبکه، نرخ انتقال داده و نوع پروتکل مسیریابی در شکست مسیر ارزیابی شده است. مدل پتری ارائه شده که الهام گرفته از مدل‌های مارکوف ارائه شده در [۵۶] می‌باشد با محاسبه تعداد گام لازم جهت دستیابی به مقصد (n)، از n قطعه مدل پتری تشکیل شده است. در هر قطعه از شبکه پتری نرخ خروج گره همسایه‌ای که به‌عنوان گره بعدی در مسیر شناخته می‌شود به همراه نرخ بازیابی گره دیگری به‌عنوان گره جایگزین

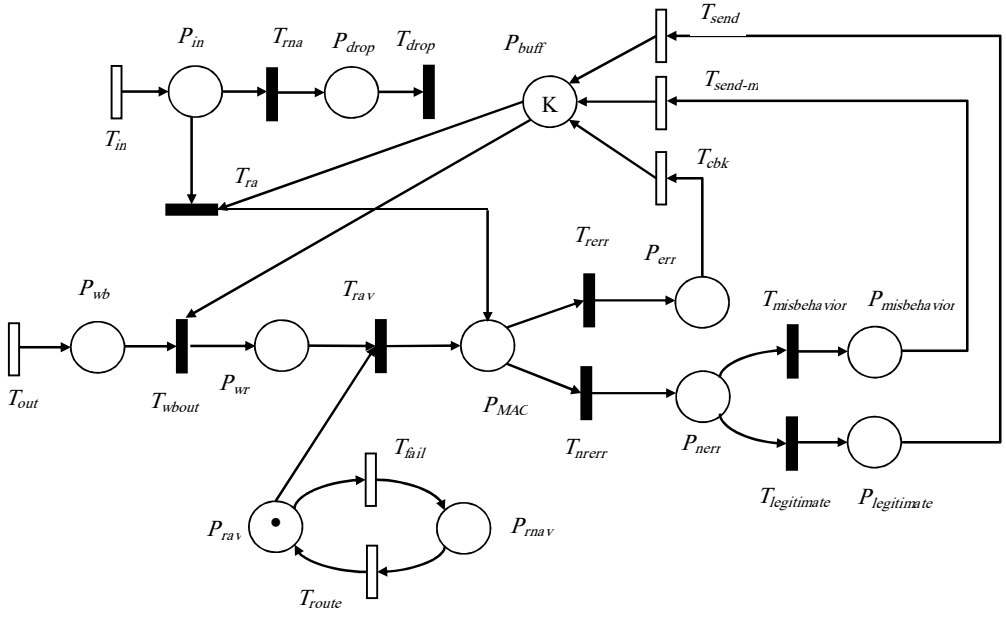
[1] Path connection availability

محاسبه شده است. در نهایت، خروجی مدل شبکه پتری ارائه شده در این تحقیق استخراج معیارهایی چون احتمال از دست رفتن مسیر و نرخ از دست رفتن و بازیابی مسیر بوده است.

پس از وقوع یک شکست، یک فرایند مسیریابی جدید موردنیاز است که با استفاده از گذار T_{route} نشان داده شده است. زمان موردنیاز برای این گذار، از مدل فرایند مسیریابی معرفی‌شده در بخش ۴-۲-۲ محاسبه می‌شود. مجموعه المان‌های (P_{rnav} ,P_{rav} ,T_{fail} ,T_{route} ,T_{rav}) به‌گونه‌ای عمل می‌کنند که بسته تنها زمانی برای ارسال به لایه MAC فرستاده شود که مسیر قابل‌دسترسی برای آن موجود باشد. بسته تولیدشده باید از طریق مسیری که توسط فرآیند مسیریابی تولید شده است به گره بعدی در مسیر ارسال شود. این کار توسط لایه پیوند داده انجام می‌شود که مسئول ایجاد یک ارتباط یک گامه مطمئن در یک فضای همسایگی می‌باشد. IEEE 802.11 DCF به‌عنوان یک پروتکل پیوند داده مسئول هماهنگی گره‌ها در این لایه می‌باشد. علی‌رغم تکنیک‌های پیشرفته‌ای که برای جلوگیری از برخورد در ارسال داده در این پروتکل پیش‌بینی‌شده است، ممکن است در کانال مشترک موجود در یک ناحیه همسایگی تصادم رخ دهد. احتمال مرتبط با این احتمال که با استفاده از ساختار انتخاب (T_{err}-T_{nerr}) نشان داده شده است با استفاده از رابطه ۴-۱۴ از مدل جزئی گره‌ها برای لایه پیوند داده معرفی‌شده در بخش ۴-۱-۳ محاسبه شده است. T_{err} نشان‌دهنده حالتی است که گره نمی‌تواند داده خود را با موفقیت منتقل در لایه پیوند داده ارسال کند و احتمال آن برابر (۱-δ) خواهد بود و T_{nerr} نیز وضعیتی را نشان می‌دهد که لایه پیوند داده موفق به ارسال داده از طریق کانال خواهد شد و احتمال آن برابر δ می‌باشد.

همان‌طور که در ابتدای این بخش به‌طور مختصر و در فصل ۲ به‌طور کامل توضیح داده شد، از مصائب دیگری که لایه شبکه در شبکه‌های موردی سیار به آن دچار است آلوده شدن مسیر به یک یا چند گره متخاصم می‌باشد. گره متخاصم ممکن است به‌عنوان یک حمله سیاه‌چاله عمل کند و بسته‌های RREP جعلی را به سمت بسته‌های RREQ دریافتی ارسال کند که این بسته‌های جعلی دارای تعداد

گام کمینه و شماره توالی بزرگ می‌باشند که باعث تطمیع گره صادرکننده RREQ برای ارسال داده از مسیر گره متخاصم خواهد شد. گره متخاصم نیز درنهایت اقدام به حذف بسته‌های داده ارسالی از مسیر خود خواهد کرد. به‌عنوان استراتژی دیگر در حمله نوع انهدام بسته‌ها، گره متخاصم در فرآیند مسیریابی به‌درستی عمل می‌کند و پس از قرار گرفتن در مسیر ایجادشده از گره مبدأ به گره مقصد، تنها بسته‌های داده دریافتی را حذف می‌کند. توضیحات مفصل راجع به هر یک از حملات در بخش ۴-۴-۲ داده‌شده است.



شکل ۴-۳: مدل SRN برای فرآیند جریان داده‌ها

در مدل ارائه شده با این فرض که تعدادی گره متخاصم در فضای شبکه همراه با سایر گره‌های مشروع در تعامل هستند مسیر به دست آمده از گذار T_{route} ممکن است به گره متخاصمی آلوده‌شده باشد یا خیر. این مورد توسط گذار $T_{misbehavior}$ در مدل نشان داده‌شده و احتمال مرتبط با آن از مدل فرآیند

مسیریابی که در بخش ۴-۲-۲ معرفی‌شده به دست خواهد آمد. T_{send} و $T_{send\text{-}m}$ به ترتیب به زمان موردنیاز برای تحویل یک بسته به گره بعدی معتبر و متخاصم از طریق لایه پیوند داده اشاره می‌کند.

زمان اجرای مرتبط با این دو گذار یکسان بوده که به دلیل مسائل مدل‌سازی توسط گذارهای مجزا نشان داده شده‌اند. T_{send} و $T_{send\text{-}m}$ با استفاده از رابطه ۴-۳۵ از مدل برهم‌کنش گره‌ها ارائه شده در بخش ۴-۱-۲ به دست می‌آید. در استخراج این رابطه از قانون Little استفاده شده است. T_{CBK} نیز ناظر به زمان موردنیاز جهت شناسایی خطای ارسال می‌باشد که توسط رابطه ۴-۳۶ به دست می‌آید.

$$T_{Send} = \frac{\mathrm{N-m(P_N)}}{\mathrm{Thr(T_{DS})}} \qquad (۳۵\text{-}۴)$$

$$T_{CBK} = (T_{DIFS} + T_{Backoff} + T_{timeout}) \times MRL \qquad (۳۶\text{-}۴)$$

بر اساس پروتکل مسیریابی AODV، درصورتی‌که گره‌ای بسته داده‌ای را دریافت کند که مسیر منقضی نشده‌ای برای آن نداشته باشد، بسته موردنظر بلافاصله دور انداخته می‌شود. از بین رفتن مسیر موجود جهت یک جهت یک بسته می تواند به علت های مختلفی مانند حرکت گره ها و از دست رفتن قابلیت اعتماد اتصال بین گره‌های موجود در مسیر باشد. دور انداخته شده در غیر این صورت بسته به لایه MAC تحویل شده تا به گره بعدی در مسیر موجود به سمت مقصد تحویل داده شود. این دو رویداد توسط ساختار انتخاب موجود از گذارهای T_{ra} و T_{rna} نشان داده شده‌اند. برای بدست آوردن احتمال مرتبط با این گذارها باید به این مسأله توجه داشت که از دست رفتن مسیر در یک شبکه موردی سیار تابع مستقیمی از قابلیت اعتماد شبکه می باشد. قابلیت اعتماد شبکه نیز بطور مستقیم تابعی از قابلیت اعتماد گره‌ها و اتصالات مابین آن‌ها می باشد. بنابراین در صورتی که قابلیت اعتماد یک شبکه G با n گره را در نظر بگیریم، قابلیت اعتماد کل شبکه بصورت رابطه ۴-۳۷ تعریف خواهد شد. که در آن R نشان دهنده قابلیت اعتماد گره و L نیز معرف قابلیت اعتماد اتصالات مابین آن‌ها است.

$$2\mathrm{TR(G)} = \mathrm{f}(R_i, L_i) \;\; i = 1 \dots n \qquad (۳۷\text{-}۴)$$

در صورت وجود m گره در مسیر مابین گره‌های مبدأ و مقصد، احتمال برقراری بین آن‌ها از رابطه ۴-۳۸ محاسبه خواهد شد.

$$P(route_i == 1) = R^m.L^{m-1} \qquad (۳۸-۴)$$

لذا با فرض وجود k مسیر فعال از گره مبدأ به مقصد، مقدار نهایی قابلیت اعتماد یک همبندی c از میان C همبندی ممکن برای یک شبکه برابر رابطه ۴-۳۹ خواهد بود. و در نهایت نیز مقدار نهایی قابلیت اعتماد یک شبکه از رابطه ۴-۴۰ بدست خوهد آمد.

$$2TR(c) = \sum_{i=1}^{k} P(route_i == 1) \qquad (۳۹-۴)$$

$$2TR = \frac{\sum_{c=1}^{C}\sum_{i=1}^{K} P(route_i==1)}{C} \qquad (۴۰-۴)$$

با پیچیده تر شدن و بزرگ شدن ابعاد شبکه امکان محاسبه قابلیت اطمینان مسیر با در نظر گرفتن تمام همبندی های ممکنه میسر نبوده است. لذا در این مرحله با استفاده از شبیه سازی مونت کارلو از یک رویکرد تصادفی جهت محاسبه قابلیت اعتماد شبکه استفاده شده است. روش شبیه سازی مونت کارلو با نمونه برداری تصادفی از فضای ورودی مساله در اجراهای با تعداد بالا، انجام محاسبات مربوطه و میانگیری از نتایج سعی در تقریب نتایج شبیه سازی به مقدار واقعی را دارد. مراحل انجام کار براساس این روش به شرح ذیل می باشد. در این روال فرض می شود گره ۱ بعنوان گره فرستنده عمل کند و گره n نیز بعنوان گره گیرنده.

۱- تعیین مقدار حد آستانه مقدار برای L و R

در تعیین مقدار R با توجه به دخیل بودن موارد زیادی در مقدار آن با رصد مقادیر بدست آمده از شبیه سازی مشخص شد که یک گره بطور متوسط در ۸۵٪ از طول عمر شبکه فعال بوده است. همچنین برای محاسبه مقدار حد آستانه L جهت وجود اتصال بین گره‌ها این مقدار دارای نسبت مستقیمی با شعاع همسایگی گره‌ها و نسبت معکوسی با مقدار یک بعد از فضای حرکت

گره ها دارد. لذا مقدار حد آستانه L براساس رابطه ۴-۴۱ محاسبه خواهد شد. که در این رابطه R_i برابر شعاع انتقال یک گره و a نیز برابر طول یک بعد از فضای حرکت گره‌های شبکه می‌باشد.

$$L = \frac{R_i}{a} \qquad (۴۱-۴)$$

۲- بطور تکراری مراحل ۳ تا ۵ انجام بده

۳- ایجاد بردارد OPR(n) بطور تصادفی برای مقدار آستانه قابلیت اعتماد گره‌ها برای n گره موجود در شبکه

۴- ایجاد ماتریس اتصال (Link) براساس مقدار بدست آمده از بردار OPR(n) و مقدار بدست آمده برای T. در ایجاد ماتریس اتصال (Link) از روال شرطی زیر استفاده می شود.

If (*opr(i)=1&opr(j)=1) &(a random number <=T)*
then
Link(i,j)=Link(j,i)=1

۵- اجرای روال BFS(Link) برای محاسبه route(r) براساس روال زیر

If (*visited(destination)=true)* then
route(r)= 1
Else
route(r)=0

۶- بدست آوردن مقدار نهایی 2TR براساس رابطه۴-۴۲

$$2TR = \frac{\sum_{i=1}^{T} route(t)}{T} \qquad (۴۲-۴)$$

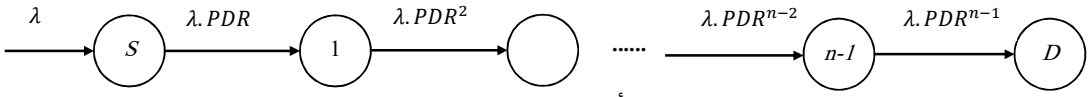
گذار T_{in} ترافیک ورودی بسته داده را نشان می‌دهد که به گره جاری رسیده است. نرخ مربوط به این گذار، تابعی از نرخ ترافیک داده خروجی ایجادشده توسط یک گره مبدأ (λ) می‌باشد. ترافیک اولیه

داده از گره مبدأ تولید می‌شود که این نرخ در مقدار نسبت تحویل داده[1] هر گره در طول مسیر از مبدأ تا مقصد ضرب می‌شود. این روند در شکل ۴-۴ نشان داده شده است. برای محاسبه نرخ فعالیت گذار T_{in}، لازم است تا ضریب نرخ تحویل بسته برای تمام گره‌های موجود در مسیر به نسبت کل گره‌های شبکه متوسط گیری شود. با داشتن تعداد n گام از مبدأ تا مقصد، نرخ فعال شدن گذار T_{in} از رابطه ۴-۳۷ به دست می‌آید که در آن s تعداد گره‌های مبدأ، λ نرخ فعال شدن گذار T_{out}، M تعداد کل گره‌ها و PDR نسبت تحویل بسته می‌باشد که توسط رابطه ۶-۳ محاسبه می‌شود. توضیحات مربوط به نحوه محاسبه PDR در بخش ۶-۳ ارائه خواهد شد.

$$rate(T_{in}) = \frac{S.\lambda.(PDR+PDR^2....+PDR^{n-1})}{M} \qquad (۴۳-۴)$$

۴-۲-۱-۱- محاسبه تعداد متوسط گام پیموده شده برای رسیدن بسته از مبدأ به مقصد

برای محاسبه n تعداد گام متوالی برای رسیدن از گره مبدأ به گره مقصد با الهام از مطالعات انجام شده در مراجع [۶۵ و ۶۷] از یک رویکرد تکراری استفاده شده است. در این رویکرد با محاسبه متوسط فاصله بین گره‌های مبدأ و مقصد و همچنین متوسط فاصله بین دو گره متوالی در مسیر انتقال داده، مقدار n محاسبه می‌شود. توجه به ماهیت اکثر الگوریتم‌های مسیریابی در شبکه‌های موردی سیار که سعی در پیدا کردن مسیری با حداقل تعداد گام موردنیاز هستند، در رویکرد انجام شده در این تحقیق نیز سعی شده تا این مورد لحاظ گردد. همچنین محاسبات انجام شده با فرض تبعیت گره‌ها از مدل حرکتی RWP بوده است.



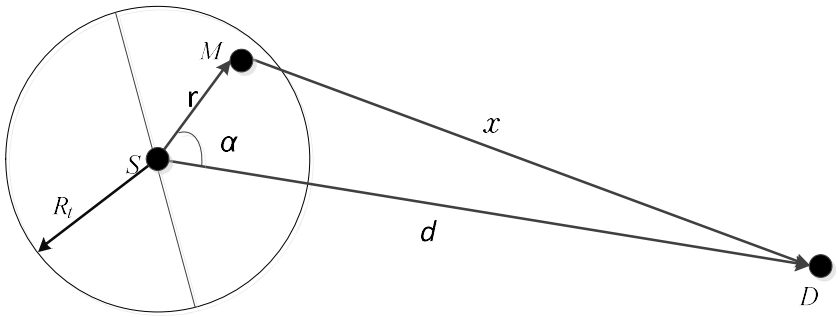
شکل ۴-۴: نرخ ترافیک داده اولیه (λ) از گره مبدأ تولید می‌شود که این نرخ در مقدار نسبت تحویل داده هر گره در طول مسیر از مبدأ تا مقصد ضرب می‌شود.

[1] Packet delivery ratio (PDR)

در تکنیک بکار رفته، ابتدا لازم است تا متوسط فاصله بین دو گره مبدأ و مقصد در یک شبکه با ابعاد a محاسبه شود. همان‌طور که در شکل ۴-۵ نشان داده‌شده است این فاصله با نماد d نشان داده‌شده که بر اساس رابطه ۴-۴۴ برگرفته از مرجع [۶۶] محاسبه خواهد شد.

$$d = \left(\frac{11}{350}\ln\left(\sqrt{2}+1\right) + \frac{28083}{750750}\sqrt{2} + \frac{19064}{375375}\right).a \qquad (۴۴-۴)$$

در گام بعدی متوسط فاصله میان گره مبدأ با گره متوالی بعدی در مسیر محاسبه خواهد شد. رابطه به دست آمده با فرض یافتن گره‌ای که بیشترین فاصله را در میان گره‌های همسایه یک گره دارد عمل می‌کند که این راهبرد منجر به محاسبه کمترین تعداد گام منتهی به مقصد می‌شود. این فاصله در شکل ۴-۵ با استفاده از نماد r نشان داده‌شده است که بر اساس [۶۴] به‌صورت رابطه ۴-۴۵ محاسبه خواهد شد. در تحقیقات انجام شده در این مرجع با مطالعه اثرات پارامترهای شبکه نظیر تراکم گره‌ها، اندازه محدوده شبکه و محدوده انتقال مقدار این فاصله محاسبه شده است. در این رابطهn_r نشان‌دهنده تعداد گره‌های بالقوه به‌منظور انتخاب گره بعدی در مسیر منتهی به مقصد می‌باشد که در اینجا فرض است که برابر نصف تعداد گره‌های همسایه یک گره باشد و از رابطه ۴-۲۲ محاسبه خواهد شد.



شکل ۴-۵ فاصله اقلیدسی ارسال داده از گره مبدأ S به گره مقصد D با استفاده از گره میانی حائل M

همانطور که از این رابطه برمی‌آید با افزایش R_t که همان شعاع انتقال یک گره محسوب می‌شود و n_r، مقدار این فاصله افزایش خواهد یافت که درنهایت منجر به کاهش تعداد گام خواهد شد.

$$r = \frac{2n_r}{2n_r+1}.R_t \qquad (۴۵-۴)$$

برای محاسبه مقدار فاصله باقیمانده جهت رسیدن به مقصد (x)، همان‌طور که در شکل ۴-۵ نشان داده شده است دامنه نوسان زاویه گره متوالی بعدی در مسیر رسیدن به مقصد برابر ($-\frac{\pi}{2} \leq \alpha \leq \frac{\pi}{2}$) می‌باشد. بنابراین تابع احتمال مقدار فاصله باقیمانده جهت رسیدن به مقصد (x) با در نظر گرفتن زاویه متناظر α مطابق رابطه ۴-۴۶ خواهد بود.

$$f_\alpha(\alpha) = \frac{1}{\pi} \ (-\frac{\pi}{2} \leq \alpha \leq \frac{\pi}{2}) \qquad (۴۶-۴)$$

با انتگرال‌گیری از $f_\alpha(\alpha)$ و جایگزینی α از طریق رابطه $X = \sqrt{d^2 + r^2 - 2Xrcos(\alpha)}$ تابع تجمعی (x) برابر رابطه ۴-۴۷ خواهد بود. با اعمال مشتق روی این تابع مقدار تابع احتمال کلی x برابر رابطه ۴-۴۸ می‌باشد

$$F_X(X) = \frac{2}{\pi}\arccos\left(\frac{d^2+r^2+X^2}{2dr}\right) \qquad (۴۷-۴)$$

$$f_X(X) = \frac{2X}{\pi dr\sqrt{1-\left(\frac{d^2+r^2+X^2}{2dr}\right)^2}} \qquad (۴۸-۴)$$

درنهایت مقدار مورد انتظار x با انتگرال‌گیری از تابع احتمال آن در سطح $d-r$ تا$d^2 - r^2$ بدست خواهد آمد که مراحل کار در ذیل نشان داده شده است که نهایتاً طبق رابطه ۴-۴۹ خواهد بود.

$$E(x) = \int_{d-r}^{\sqrt{d^2+r^2}} x.f(x)\,d(x) = \int_{d-r}^{\sqrt{d^2+r^2}} \frac{2}{\pi dr} \times \frac{x^2}{\sqrt{1-\left(\frac{d^2+r^2-x^2}{2dr}\right)^2}}\ d(x)$$

با استفاده از بسط $(1-x)^{-\alpha} = \sum_{n=0}^{\infty} \frac{\Gamma(n+\alpha)}{n!\Gamma(\alpha)} \times x^n$ داریم

$$E(x) = \frac{2}{\pi dr} \times \int_{d-r}^{\sqrt{d^2+r^2}} x^2 \left(1-\left(\frac{d^2+r^2-x^2}{2dr}\right)^2\right)^{-1/2} d(x)$$

با شرط $-1 < \frac{d^2+r^2-x^2}{2dr} < 1$ داریم

$$E(x) = \frac{2}{\pi dr} \times \int_{d-r}^{\sqrt{d^2+r^2}} x^2 \sum_{n=0}^{\infty} \frac{\Gamma(n+1/2)}{n!\,\Gamma(1/2)} \cdot \left(\frac{d^2+r^2-x^2}{2dr}\right)^{2n} . d(x)$$

$$E(x) = \frac{2}{\pi dr(2dr)^{2n}} \times \sum_{n=0}^{\infty} \frac{\Gamma(n+1/2)}{n!\,\Gamma(1/2)} \times \int_{d-r}^{\sqrt{d^2+r^2}} x^2 (d^2+r^2-x^2)^{2n} d(x)$$

با استفاده از تغییر متغیر $\begin{cases} x = v \quad , \quad dx = dv \\ v = -\frac{1}{2(2n+1)}(d^2+r^2-x^2)^{2n+1} \end{cases}, x(d^2+r^2-x^2)^{2n}dx = dv$

داریم:

$$E(x) = \frac{2}{\pi\sqrt{\pi}.rd.(2dr)^{2n}} \times \sum_{n=0}^{\infty} \frac{\Gamma(n+1/2)}{n!} \times \frac{(d-r).(2dr)}{2(2n+1)} + \frac{1}{2(2n+1)} \int_{d-r}^{\sqrt{d^2+r^2}} (d^2+r^2-x^2)^{2n+1} d(x)$$

در نهایت مقدار مورد انتظار x از رابطه (۴-۴۹) محاسبه خواهد شد.

$$E(x) = \frac{2}{\pi\sqrt{\pi}.rd.(2dr)^{2n}} \times \sum_{n=0}^{\infty} \frac{\Gamma(n+1/2)}{n!} \times \left(2dr(d-r) + \frac{\sqrt{\pi}\,\Gamma(2n+2)(d^2+r^2)^{2n+3/2}}{2\Gamma(2n+\frac{5}{2})}\right)$$

(۴-۴۹)

مراحل الگوریتم تا زمانی که مقدار $x \le R_t$ ادامه خواهد یافت و در هر مرحله به اندازه یک واحد به مقدار تعداد گام اضافه خواهد شد

خلاصه روال صورت گرفته برای محاسبه تعداد گام برای ارسال داده از مبدأ به مقصد در یک شبکه با ابعاد a به شرح ذیل است

۱. ورودی: a، N و R_t

۲. تعیین مقدار d بر اساس رابطه ۴-۴۴
۳. $Hop\_count=0$
۴. تکرار کن
۵. تعیین مقدار x بر اساس رابطه ۴-۴۹
۶. $d = d - x$
۷. $Hop\_count= Hop\_count+1$
۸. تا زمانی که $d \leq R_t$

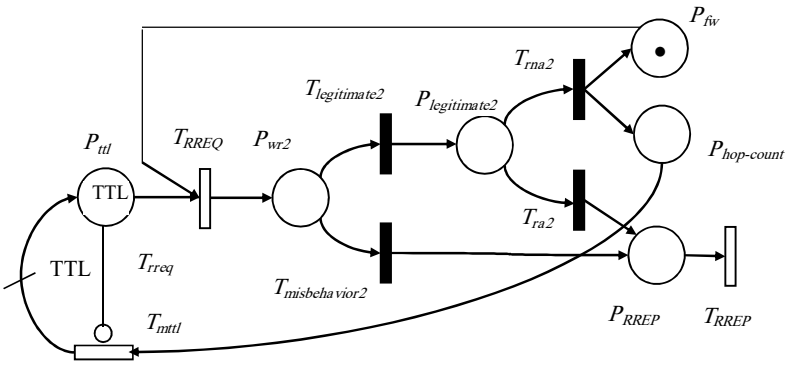
۴-۲-۲-مدل SRN برای فرآیند مسیریابی

در این بخش رفتار پروتکل مسیریابی AODV مدل شده است. همان‌طور که در بخش ۲-۴-۲ توضیح داده شده، در پروتکل مسیریابی AODV فرآیند مسیریابی با انتشار پیغام‌های RREQ به گره‌های همسایه و با یک شمارنده TTL که محدوده انتشار RREQ را نشان می‌دهد آغاز می‌شود. این شمارنده با هر بار انتقال RREQ از یک گره به گره دیگر کاهش می‌یابد. RREQ از میان گره‌ها عبور می‌کند تا به مقصد برسد. این فرآیند با رسیدن به گره‌ای که مسیر معتبری به‌سوی مقصد دارد خاتمه می‌یابد. مانند مدل جریان داده، مدل فرآیند مسیریابی نیز باید عملکرد گره‌های مهاجم را همانند عملکرد صحیح گره‌های مشروع نشان دهد. روند انجام کار که تحت عنوان مدل فرآیند مسیریابی نامیده شده در شکل ۴-۶ نشان داده‌شده است. همان‌طور که در بخش ۲-۴-۲ به‌طور مفصل توضیح داده شد هر درخواست RREQ حاوی یک ویژگی به نام TTL Number می‌باشد که محدوده گسترش بسته RREQ را در شبکه مشخص می‌کند و بر اساس یک رابطه زمانی گره مبدأ در انتظار بسته RREP تا آن بازه زمانی می‌ماند. در صورت عدم حصول نتیجه و دریافت نکردن RREP، گره مبدأ مجدداً اقدام به ارسال بسته RREQ این بار با TTL Number بیشتر (معمولاً دو برابر مقدار قبلی) خواهد نمود. این فرآیند (اضافه کردن مقدار TTL Number) تا زمانی ادامه پیدا می‌کند که به یک مقدار حدی برای

ویژگی TTL[1] برسیم که در آن صورت بسته داده دور انداخته خواهد شد و مشخصات آن از بافر تمام گره‌های درگیر پاک می‌شود. شروع مقدار TTL[2] معمولاً با مقدار ۲ می‌باشد و حد پایان آن ۷ است. بر اساس عملکرد پروتکل مسیریابی AODV همان‌طور که در شکل ۴-۶ نشان داده‌شده است در ابتدا تعداد TTL نشانه در مکان P_{ttl} قرار می‌گیرد که مشخص‌کننده محدوده انتشار بسته‌های RREQ می‌باشد. هر بار فعال شدن گذار T_{rreq} نشانگر آن است که بسته RREQ از طرف یک گره ارسال شده است که با فعال شدن آن یک واحد از مقدار TTL کاهش می‌یابد. باهدف قرار دادن حمله سیاه‌چاله این احتمال وجود دارد که یک یا چند گره متوالی به‌عنوان گره بدرفتار عمل کنند و برای RREQ دریافت شده RREP جعلی ارسال کنند. بنابراین با انتقال نشانه به مکان P_{wr2} احتمال اینکه گره بعدی یک گره متخاصم و یا مشروع باشد توسط ساختار انتخاب ($T_{misbehavior2} - T_{legitimate2}$) نشان داده می‌شود. در صورت متخاصم بودن گره بعدی، پیغام RREP سریعاً از طرف آن ارسال می‌شود. در غیر این صورت گره مشروع بعدی در دسترس بودن مسیر را در جدول مسیریابی خود بررسی می‌کند.

در صورت موجود بودن مسیر هم پیغام RREP از طرف این گره ارسال خواهد شد. در غیر این صورت فرآیند مسیریابی توسط گره‌های بعدی ادامه می‌یابد. مکان $P_{hop-count}$نیز به‌منظور محاسبه تعداد گام‌های طی شده تا رسیدن به گره مقصد و یا گره‌ای که از آن اطلاع دارد، استفاده خواهد شد. همچنین تابع نگهبان روی گذار TRREQ تعبیه شده که سبب می‌شود این گذار تنها زمانی فعال شود که هیچ نشانه‌ای در یکی از مکان‌های P_{wr2} ،P_{fw} ،$P_{legitimate}$ و یا P_{RREP} باقی نمانده باشد.

[1] TTL threshold
[2] TTL Start



شکل ۴-۶: مدل SRN فرآیند مسیریابی بر اساس پروتکل AODV

احتمال فعال شدن مربوط به انتقال‌های $T_{legitimate2}$ و $T_{misbehavior2}$ ارتباطی مستقیم با نسبت تعداد گره‌های بدرفتار در یک ناحیه همسایگی نسبت به کل گره‌های موجود در یک همسایگی دارد. با فرض انتخاب RWP به‌عنوان مدل حرکتی گره‌ها، تعداد گره‌های مشروع (N) و متخاصم (N_m) موجود در یک ناحیه همسایگی بر اساس معادله ۴-۲۲ محاسبه خواهد شد. درنتیجه احتمال مرتبط با فعال شدن گذارهای $T_{misbehavior2}$ و $T_{legitimatet2}$ بر اساس رابطه ۴-۵۰ خواهد بود.

$$T_{misbehavior2} = \frac{N_m}{N}$$
$$T_{legitimatet} = 1 - T_{misbehavior2} \qquad (۵۰-۵)$$

درصورتی‌که تمام گره‌های موجود در یک همسایگی مشروع باشند، این امکان وجود دارد که یک یا چند گره مسیری به سمت مقصد داشته باشند و بسته RREP حاوی آدرس گره مقصد را در قبال RREQ دریافتی به سمت مقصد ارسال کنند. احتمال مرتبط با این موضوع توسط ساختار انتخاب (T_{rna} - T_{ra}) نشان داده شده است که مقدار آن ارتباط مستقیمی با تعداد گره‌های موجود در یک همسایگی و اندازه جدول مسیریابی آن‌ها دارد. این موضوع توسط معادله ۴-۵۱ نشان داده شده است.

$$\Pr(Trna2) = \left(1 - \frac{(RT\_Size)}{M}\right)^N \qquad (۵۱-۴)$$

واضح است که $\Pr(Tra2)$ برابر $1 - \Pr(Trna)$می‌باشد. RT_size ناظر بر اندازه جدول مسیریابی است که مقدار آن از مرجع [۶۸] استخراج شده است. بر اساس مطالعات موجود در این مرجع در

پروتکل‌های واکنشی درصورتی‌که M گره در شبکه داشته باشیم، اندازه جدول مسیریابی هر گره از رابطه حدودی $\log_2 M$ خواهد بود. همان‌طور که می‌دانیم پروتکل مسیریابی AODV برای ارسال بسته‌های RREQ از روش پخش همگانی استفاده می‌کند. بنابراین زمان مربوط به اجرای گذار T_{RREQ} برابر است با زمان موردنیاز برای پخش همگانی یک بسته RREQ در کانال عمومی که از استاندارد IEEE 802.11 DCF استخراج خواهد شد. اما با توجه به ارسال تک‌پخشی بسته‌های RREP، پروتکل AODV مجبور به استفاده از روش ساده دست تکانی دومرحله‌ای پایه[1] برای دسترسی به کانال است.. در این روش، یک گره پس‌ازآنکه به فاصله یک DIFS، کانال را آزاد احساس کند به‌سادگی بسته‌های کوچکی از داده و یا بسته‌های کنترلی را ارسال می‌کند. همراه با دریافت بسته از سوی فرستنده، گره گیرنده پس‌ازآنکه به فاصله یک SIFS، کانال را آزاد احساس کند یک فریم ACK به‌منظور اعلام دریافت موفقیت‌آمیز می‌فرستد. بنابراین زمان ارسال یک RREP یک گامه مطابق رابطه ۴-۵۲ خواهد بود.

$$Time(T_{RREP-Hop}) = \tau_{DIFS} + \tau_{SIFS} + \tau_{ACK} + \tau_{control\ packet} \qquad (۵۲-۴)$$

بنابراین با توجه به اینکه پیغام RREP باید از تعداد گره‌های مابین گره مبدأ تا گره مقصد و یا گره‌ای که اطلاعی از مقصد دارد بگذرد لذا، رابطه زمانی کلی T_{RREP} برابر معادله ۴-۵۳ خواهد بود. که در آن $\mathrm{m}(P_{hop-count})$ برابر متوسط تعداد گام بین گره مبدأ و گره مقصد و یا گره‌ای می‌باشد که اطلاع از آدرس آن دارد. این مقدار از مدل SRN فرآیند مسیریابی استخراج خواهد شد.

$$Time(T_{RREP}) = Time(T_{RREP-Hop}) \times \mathrm{m}(P_{hop-count}) \qquad (۵۳-۴)$$

همان‌طور که در بخش قبل مطرح شد زمان فعالیت گذار T_{route} در مدل SRN جریان داده (زمان لازم جهت فرآیند مسیریابی) از مدل SRN فرآیند مسیریابی استخراج خواهد شد. با استفاده از قانون little

[1] Basic acess

[۶۵]، زمان سپری‌شده برای فعال شدن این گذار با استفاده از رابطه ۴-۵۴ به دست خواهد آمد. $\mathrm{m}(P_{ttl})$ برابر متوسط تعداد نشانه‌های موجود در مکان P_{ttl} و $Thr(T_{RREQ})$ نیز توان گذردهی گذار T_{RREQ} می‌باشد.

$$Time(T_{route}) = \frac{TTL - \mathrm{m}_{ttl})}{Thr(T_{RREQ})} + T_{RREP} \qquad (۵۴-۴)$$

همچنین احتمال مربوط به ساختار انتخاب ($T_{legitimate}$- $T_{misbehavio}$) در مدل جریان داده که به احتمال آلوده شدن یک مسیر توسط گره‌های متخاصم اشاره می‌کند برحسب نوع حمله می‌تواند متفاوت باشد. برای حمله سیاه‌چاله، احتمال آلوده شدن یک مسیر به یک گره متخاصم ممکن است در فرآیند مسیریابی رخ دهد. احتمال مرتبط با آلوده بودن مسیر ارتباط مستقیمی با نسبت تعداد گره‌های متخاصم به کل گره‌های شبکه و همچنین طول فرآیند مسیریابی دارد. منظور از طول فرآیند مسیریابی در اینجا متوسط فاصله طی شده از گره مبدأ تا گره مقصد و یا گره‌ای می‌باشد که از آن اطلاع دارد. مقدار این فاصله برابر متوسط تعداد نشانه در مکان $P_{hop-count}$ می‌باشد. لذا احتمال مرتبط با فعال شدن گذار $T_{legitimate}$ از رابطه ۴-۵۵ محاسبه می شود. واضح است که $\Pr(T_{misbehavior}) = 1 - \Pr(T_{legitimate})$

$$\Pr(T_{legitimate}) = \left(1 - \frac{N_m}{N}\right)^{\mathrm{m}(P_{hop-count})} \qquad (۵۵-۴)$$

برای حمله انهدام بسته‌ها معادله مشابه‌ای استفاده خواهد شد، با این تفاوت که گذار $T_{misbehavior2}$ از مدل حذف شده است. چون در این نوع حمله، گره متخاصم در فرایند مسیریابی همانند یک گره مشروع عمل می‌کند اما در فرآیند انتقال داده، بسته‌های داده را منهدم می‌کند.

۴-۳- ارائه پروتکل مسیریابی امن

در تلاش دیگری در این بخش سعی شده با استفاده از ویژگی‌های ذاتی مدل شبکه پتری فازی اقدام به ارائه یک مسیریابی امن مبتنی بر پروتکل مسیریابی AODV شود. لازم به یادآوری است که مباحث

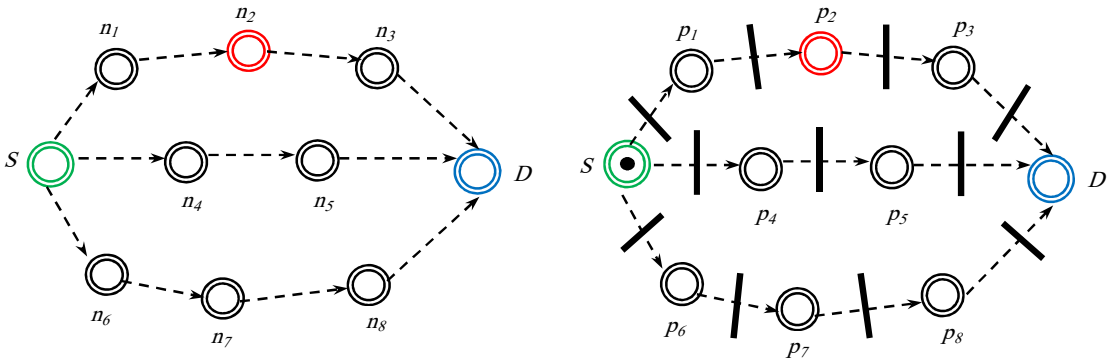
مربوط به تئوری و کارکرد مدل شبکه پتری فازی در بخش ۳-۶ ارائه شده است. به‌منظور تأمین امنیت یک پروتکل مسیریابی، دو مسئله عمده باید در نظر گرفته شوند: مسئله اول حفاظت از اطلاعات منتقل‌شده از یک گره به گره دیگر و دیگری امن ساختن کل مسیر انتقال می‌باشد. با این توضیح برای داشتن مسیری امن از طریق گره مبدأ به مقصد، دو تابع وارسی امنیت گره به گره[۱] و وارسی امنیت مسیر[۲] باید در نظر گرفته شوند. تابع وارسی امنیت گره به گره برای بر حذر شدن از رفتار گره‌های متخاصم استفاده خواهد شد. با وجوداین تابع، مسیری که در آن گره متخاصمی وجود داشته باشد قبل از رسیدن به مقصد قطع می‌شود. برای سایر مسیرها که در آن‌ها هیچ گره مخربی در آن وجود ندارد، تابع وارسی امنیت کل مسیر، اقدام به پیدا کردن امن‌ترین مسیر در میان مسیرهای ممکن خواهد نمود.

در طرح پیشنهادی، هر گره به‌عنوان مکانی در ساختار شبکه پتری فازی و ارتباط بین هر جفت از گره‌ها به‌صورت یک گذار فرض می‌شود که عامل قطعیت[۳] آن به متریک‌های قابلیت اطمینان و امنیت مسیر انتقال داده و گره‌های مرتبط با گره جاری بستگی دارد. به‌عنوان‌مثال، شکل ۴-۷ (الف) یک شبکه موردی سیار را نشان می‌دهد که شامل تعدادی گره می‌باشد. گره مبدأ با S نشان داده شده است و می‌خواهد به گره مقصد که با D نشان داده شده داده‌ای را ارسال کند. در این شبکه، در فرآیند مسیریابی و برقراری ارتباط، گره مخرب N2 می‌تواند به شیوه خصمانه شرکت کند. با استفاده از این تعریف، مدل شبکه پتری فازی از توپولوژی شبکه موجود در شکل ۴-۷ (الف) مطابق با شکل ۴-۷ (ب) خواهد بود.

[1] Node to node security verification
[2] route security verification
[3] Certainty factor

۴-۳-۱-تابع وارسی امنیت گره به گره

در تابع وارسی امنیت گره به گره، هر گره معیارهای امنیتی مرتبط با همسایگان خود که بسته‌های کنترلی و یا داده را با آن‌ها ردوبدل می‌کنند را ارزیابی می‌کند. این وارسی بر اساس استنتاج صورت گرفته از پارامترهای فازی ورودی مرتبط با گره‌های همسایه که در فرآیند مسیریابی شرکت می‌کنند انجام خواهد شد. فازی سازی در اینجا روی هر اتصال ارتباطی و یا مقادیر مرتبط با عامل قطعیت گذار معادل آن در مدل فازی پتری هم‌ارز انجام می‌شود. هر چه قابلیت اطمینان و امنیت بین هر جفت از گره‌ها بیشتر باشد، مقدار عامل قطعیت برای انتقال داده مرتبط با آن گذار بیشتر می‌شود. به این منظور، برای انتقال یک بسته داده از گره P_i به گره P_j، چهار متغیر فازی در نظر گرفته شده است (شکل ۴-۸). این متغیرها برای تعیین سطح امنیت[1] اتصال ارتباطی آن‌ها استفاده می‌شود.



شکل ۴-۷. الف) یک شبکه فرضی موردی سیار ب) مدل شبکه پتری فازی معادل شبکه

[1] Security Level (SL)

این متغیرها به‌منظور پایش کانال, پوشش تمام اثرات مرتبط با فعالیت‌های حملات معمول ازجمله سیاه‌چاله، ارسال سیل‌آسا و انهدام بسته انتخاب شده‌اند. متغیرهای استفاده شده در ادامه معرفی شده‌اند.

درصد بسته‌های داده منهدم شده[۱]: درصد بالایی از این متغیر می‌تواند نشان‌دهنده حمله انهدام بسته باشد.

نسبت تعداد RREQ های ارسالی به تعداد کل بسته‌های ارسالی[۲]: مقدار بالای این متغیر احتمال حمله ارسال سیل‌آسا را نشان می‌دهد.

نسبت تعداد RREP های ارسالی به تعداد RREQ های دریافتی[۳]: مقدار بالای این متغیر احتمال حمله سیاه‌چاله را نشان می‌دهد.

درصدی از به‌روزرسانی‌های غیرمعمول[۴]: به‌روزرسانی غیرمعمول در موارد زیر رخ می‌دهد: Pi، یک بسته RREQ از گره Pj دریافت می‌کند که شماره توالی مبدأ و یا شماره توالی مقصد کمتری نسبت به RREQ دارد که قبلاً از گره Pj دریافت کرده است. Pi یک RREQ از گره Pj دریافت می‌کند که تعداد گام کمتری نسبت به RREQ دارد که قبلاً از گره Pj دریافت کرده است.

خروجی: خروجی سیستم فازی سطح امنیت هر گره را نشان می‌دهد.

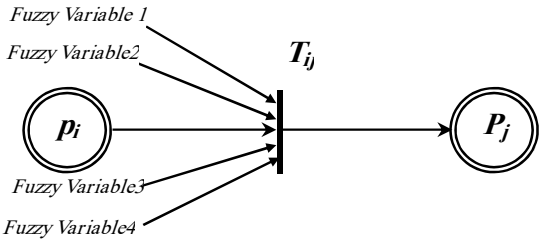
برای هر یک از متغیرهای فازی تابع عضویت، سه مجموعه فازی با عنوان پایین[۵]، متوسط[۶] و بالا[۷] در نظر می‌گیریم. محدوده مقادیر هر متغیر فازی به دلیل ویژگی‌های منحصربه‌فرد خود برای هر یک از

---

[1] Percentage of dropped data packet
[2] Proportion of number of sent RREQ to the whole number of sent packet
[3] Proportion of number of sent RREP to the number of received RREQ
[4] Percentage of abnormal updates
[5] Low
[6] Medium
[7] High

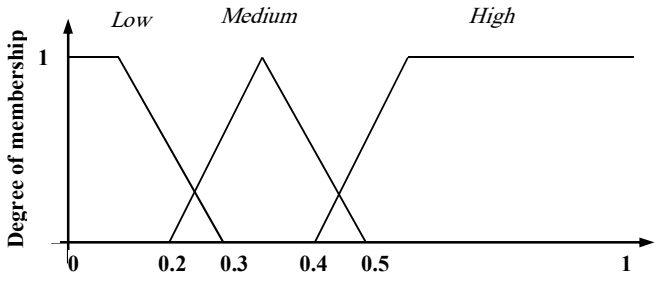
مقادیر مجموعه‌های فازی، متفاوت است. برای متغیر فازی خروجی که نشان‌دهنده سطح امنیت خروجی است، پنج مجموعه فازی با عنوان پایین‌ترین[1]، پایین[2]، متوسط[3]، بالا[4] و بالاترین[5] در نظر گرفته شده است. برای هر متغیر فازی، شکل‌های ۴-۹ تا ۴-۱۳ شکل تابع عضویت را همراه با محدوده مقادیر هر مجموعه نشان می‌دهند. این متغیرهای فازی که درواقع معرف وضعیت گره‌های شرکت‌کننده در یک ارتباط بی‌سیم هستند و به امکان فعال شدن هر گذار (اتصال) تأثیر می‌گذارند.

قوانین مرتبط با استنتاج فازی، با بررسی اطلاعات شبکه استخراج خواهند شد. با بررسی قوانین فازی مشخص شد که هر متغیر فازی تأثیر مشابه‌ای بر روی شبکه دارد به همین منظور برای تولید قوانین در اینجا از یک رویکرد کمی استفاده شده است که در آن تعداد متغیرهای فازی در هر یک از مجموعه‌های فازی (پایین‌ترین، پایین، متوسط، بالا و بالاترین) مبنای تولید قانون قرار گرفته است.

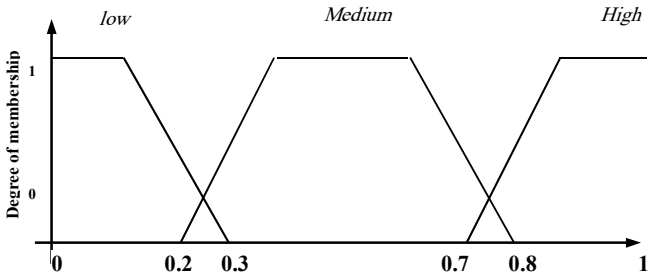


شکل ۴-۸. چهار متغیر فازی برای فعال شدن اتصال ارتباطی (گذار) بین دو گره فعال هستند

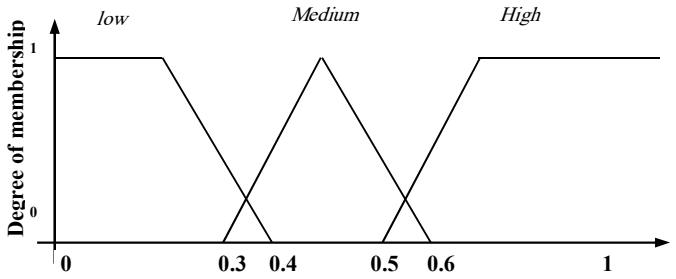
[1] Lowest
[2] Low
[3] Medium
[4] High
[5] Highest



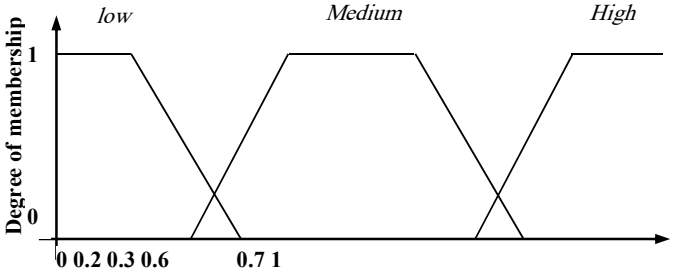
شکل ۴-۹ تابع عضویت فازی برای متغیر فازی، درصد بسته‌های داده منهدم شده



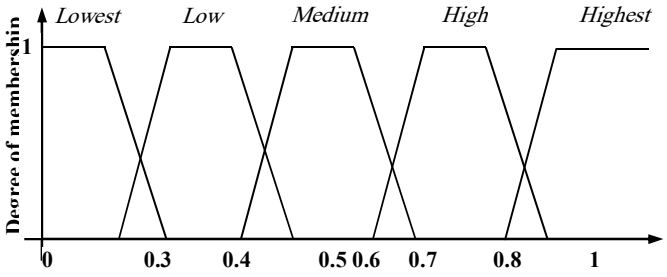
شکل ۴-۱۰ تابع عضویت فازی برای متغیر فازی، نسبت تعداد RREQ های ارسالی به تعداد کل بسته‌های ارسالی



شکل ۴-۱۱. تابع عضویت فازی برای متغیر فازی، نسبت تعداد RREP های ارسالی به تعداد RREQ های دریافتی



شکل ۴-۱۲ تابع عضویت فازی برای متغیر فازی، درصد به‌روزرسانی‌های غیرمعمول



شکل ۴-۱۳ تابع عضویت فازی برای متغیر فازی، خروجی

برای هر متغیر ورودی، نزدیک شدن به سطح بالاتر به بدتر شدن وضعیت امنیتی شبکه تفسیر شده و موجب پایین‌تر آمدن سطح متغیر فازی خروجی می‌شود. قوانین در جدول ۴-۴ ذکر شده‌اند.

برای اجتناب از ارسال و یا دریافت داده به/از گره‌های متخاصم، یک سطح آستانه امنیت توسط گره‌های مشروع اختصاص داده شده که در سطح فازی متغیر خروجی تنظیم می‌شود. این حد آستانه می‌تواند سطح متوسط و یا بالاتر در نظر گرفته شود و به معنی ارسال بسته از گره P_i به گره P_j است که گره مقصد باید در یکی از سطوح متوسط، بالا و یا بالاترین امنیت (خروجی) باشد. این امر در رویکردی دوطرفه انجام شده است و به این معنی است که گره P_j می‌تواند بسته‌های ارسالی از سوی گره P_i را بپذیرد و یا از پذیرش آن امتناع کند. انتخاب یک سطح آستانه بالاتر سبب می‌شود تا شبکه امن‌تر شود اما موانع مسیریابی در این حالت بیشتر می‌شود و ممکن است قدری تأخیر در فرآیند مسیریابی ایجاد گردد. در حملاتی مانند حمله سیل‌آسا، این استراتژی به‌عنوان پوششی امن در اطراف گره مهاجم عمل می‌کند و رفتار مخرب گره مهاجم را از کار می‌اندازد. برای مثال، در شبیه‌سازی شبکه که در شکل ۴-۱۴ نشان داده شده است گره‌های P1 و P3 برای ارسال و دریافت بسته از P2 اجتناب می‌کنند.

جدول ۴-۴: قوانین فازی اعمال‌شده روی هر اتصال ارتباطی در تابع وارسی امنیت گره به گره

قانون اول	اگر دو و یا چند متغیر فازی در سطح بالا باشند آنگاه خروجی در سطح پایین‌ترین است
قانون دوم	اگر یک متغیر فازی در سطح بالا باشد و سایر متغیرها در سطح متوسط باشند آنگاه خروجی در سطح پایین است.
قانون سوم	اگر تمام متغیرهای فازی در سطح متوسط باشند آنگاه خروجی در سطح متوسط است.
قانون چهارم	اگر دو و یا سه متغیر فازی در سطح متوسط باشند و سایر متغیرها در سطح پایین باشند آنگاه خروجی در سطح متوسط است.
قانون پنجم	اگر سه متغیر فازی در سطح پایین باشند و سایر متغیرها در سطح متوسط باشند آنگاه خروجی در سطح بالا است.
قانون ششم	اگر تمام متغیرهای فازی در سطح پایین باشند آنگاه خروجی در سطح بالاترین است.

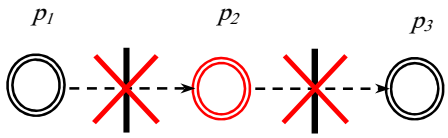
۴-۳-۲-تابع وارسی امنیت مسیر

در مسیرهایی که از گره مبدأ تا مقصد آن شامل هیچ گره متخاصمی نباشد رویکردی برای پیدا کردن امن‌ترین مسیر مورد نیاز است. برای استنتاج میزان امن بودن یک مسیر، تمام گره‌های موجود در آن باید تأثیر مشابه‌ای بر روی مسیر داشته باشند. همچنین، تأثیر منفی یک گره ناامن نباید توسط گره‌های امن موجود در یک مسیر پوشش داده شود. برای پرداختن به این استراتژی و برای انجام این تابع، می‌توان از مشخصه α به‌عنوان یک ویژگی مهم در سیستم شبکه پتری فازی استفاده کرد. بدین منظور در هر انتقال ایجاد شده از سوی تابع وارسی امنیت گره به گره، مقدار α با توجه به معادله ۴-۴۹ تغییر می‌کند. مسیری که گره‌های آن مقدار α نهایی بزرگ‌تری دارند نسبت به سایر مسیرها که شامل مقادیر کمتری از α هستند برتری دارد. روش‌های متفاوتی وجود دارند که توسط آن‌ها می‌توانیم برتری مقادیر کلی α را مشخص کنیم. عملگرهایی مانند جمع، میانگین و یا ضرب مقدار α می‌توانند انتخاب شوند. به نظر می‌رسد که ضرب مقدار α به‌طور واضح‌تری می‌تواند اثر گره‌ای که مقدار α

کمتری دارد را نشان دهد. با استفاده از این توضیحات، اگر تعداد n مسیر از مبدأ به مقصد وجود داشته باشد و هر مسیر شامل m گره از $n_1.....n_m$ باشد آنگاه سطح امنیتی مسیر k ام (SL_k) از رابطه ۴-۵۶ به دست می‌آید که برابر با ضرب مقادیر α برای تمام گره‌های موجود در مسیر می‌باشد. همچنین با انتخاب مسیر با بیشترین مقدار SL_k مسیر نهایی بین گره مبدأ (S) تا گره مقصد (D) مشخص خواهد شد(رابطه ۴-۵۷).

$$SL_k = \prod_{i=1}^{m} \alpha(p_i) \qquad (۵۶-۴)$$

$$SL_{S-D=} \max_{j \in R} SL_j \qquad R = \{R_1, R_2 \ldots\ldots R_n\} \qquad (۵۷-۴)$$



شکل ۴-۱۴: گره‌های P1 و P3 از طریق فعال نشدن انتقال مربوطه، برای ارسال و دریافت بسته از P2 اجتناب می‌کنند

۴-۳-۳-اصلاح پروتکل و پیاده‌سازی روش

برای پیاده‌سازی پروتکل اصلاحی، لازم است مشخصه‌های ضروری، به ساختار پروتکل مسیریابی AODV اصلی و جدول مسیریابی اضافه و عملکرد آن را به نحوی اصلاح کرد. در ذیل اصلاحات لازم جهت پیاده‌سازی روش در پروتکل AODV را شرح داده خواهد شد.

جدول همسایگی: همان‌طور که در توضیحات تابع وارسی امنیت گره به گره در بخش ۴-۳-۱ بیان شد، هر گره باید با رصد همسایگان خود که با آن‌ها ارسال و یا دریافت داده دارد متغیرهای فازی توضیح داده شده در بخش قبل را ایجاد کند. امکان اضافه نمودن این ویژگی‌ها به فرمت اصلی پروتکل مسیریابی AODV وجود نداشته و درنتیجه یک جدول جدید برای آن ایجاد شده است. این جدول که در شکل ۴-۱۵ نشان داده شده است شامل شناسه هر همسایه و مقادیر متغیرهای فازی مرتبط با آن

می‌باشد. با هر ارسال HELLO_MESSAGE در پروتکل مسیریابی AODV اصلی، این جدول نیز به‌روز خواهد شد. اگر یک گره همسایه در یک بازه زمانی از پیش تعیین‌شده به HELLO_MESSAGE پاسخ ندهد مدخل آن از هر دو جدول مسیریابی اصلی و جدول همسایگان حذف خواهد شد.

جدول مسیریابی اصلی: در جدول مسیریابی یک گره کاندید، باید سطح نهایی امنیت[1] مسیر استفاده شده را برای هر مقصدی داشته باشیم. این فیلد از طریق تابع وارسی امنیت مسیر بر اساس رابطه ۴-۴۹ محاسبه می‌شود و مقدار دقیق آن از طریق پیام RREP توسط گره مقصد و یا گره‌های میانی بازگشت داده می‌شود. فرمت تغییریافته جدول مسیریابی اصلی در شکل ۴-۱۶ (الف) نشان داده شده است.

ساختار پیام RREQ و عملکرد آن: برای انجام تابع وارسی امنیت مسیر، هر بسته RREQ باید قبل از رسیدن به مقصد یا گره‌ای که اطلاعی از مقصد داشته باشد، مقدار α جزئی تا آن گره را در خود ذخیره کند. به همین منظور ویژگی جدیدی به نام partial_ α به سرآیند هر بسته REEQ اضافه خواهد شد. در ابتدا partial_ α گره شروع‌کننده درخواست مسیر به یک مقداردهی می‌شود و سپس در هر پروسه کشف مسیر از یک گره به گره دیگر مقدار partial_ α گره گیرنده برابر با ضرب مقدار partial_ α فرستنده در عامل قطعیت اتصال مربوط به آن خواهد بود. به‌عنوان‌مثال، اگر در وضعیتی مانند شکل ۴-۸ باشیم که در آن P_i گره فرستنده و P_j گره گیرنده است مقدار partial_ α از P_j توسط معادله ۴-۵۵ به دست می‌آید. فرمت نهایی پیام RREQ در شکل ۴-۱۶ (ب) نشان داده شده است.

$$partial{-}\propto(P_j) = partial{-}\propto(P_i) \times Cf(T_{i-j}) \qquad (۵۸\text{-}۴)$$

[1] Security Level (SL)

ساختار پیام RREP و عملکرد آن: یک پیغام RREP می‌تواند از یک گره مقصد یا یک گره میانی که در آن مسیر جدیدی (شماره توالی بزرگ‌تر) به سمت مقصد وجود دارد به سمت گره مبدأ ارسال شود. درصورتی‌که گره ارسال‌کننده پیغام RREP خود مقصد باشد با محاسبه مقدار α_final از رابطه ۴-۵۶ پیام RREP را به گره مبدأ به‌صورت Unicast بازگشت خواهد داد. چنانچه گره صادر کنند پیغام RREP یک گره میانی باشد مقدار α_final برابر با مقدار آخرین $\alpha\_partial$ در RREQ دریافتی در مقدار SL موجود در جدول مسیریابی آن خواهد بود. با ارسال اولین پیام RREP به سمت مبدأ از یک گره به گره دیگر، تمام گره‌های میانی، مقدار SL را در جدول مسیریابی خود به‌روز می‌کنند. اگر این گره‌ها پیام RREP دیگری ملاقات کنند که شماره توالی آن به بزرگی قبلی باشد باید مقایسه‌ای بر روی مقدار α_final آن‌ها انجام شود.

اگر پیام جدیدتر دارای مقدار α_final بزرگ‌تری باشد آنگاه تمام گره‌های میانی و همچنین گره سازنده اطلاعات مربوط به خود را با مسیر امن‌تر که اخیراً رسیده جایگزین می‌کنند. فرمت کامل شده این پیغام در شکل ۴-۱۶ (ج) نشان داده شده است.

Neighbor ID	*Fuzzy Variable 1*	*Fuzzy Variable 2*	*Fuzzy Variable 3*	*Fuzzy Variable 4*	*Output State*
N_1					
N_4					
N_6					

شکل ۴-۱۵. قالب جدول همسایگی ایجاد شده شامل شناسه گره‌های همسایه و متغیرهای فازی مورداستفاده.

Destination IP address
Destination sequence
Hop_count
Next hop
Precursor list
Expiration time
SL

الف)

Type	Flags	Reserved	Hop_ Count
RREQ (Broadcast ID)			
Destination IP address			
Destination sequence number			
Originator IP address			
Originator sequence number			
Partial_∝			

ب)

Type	Flags	Reserved	Hop_Count
Destination IP address			
Destination sequence number			
Originator IP address			
Originator sequence number			
Final_∝			

ج)

شکل ۴-۱۶. قالب جدید الف) جدول مسیریابی و بسته‌های کنترلی ب) RREQ و ج) RREP در پروتکل اصلاحی

خلاصه مراحل پروتکل اصلاح‌شده AODV مبتنی بر شبکه پتری فازی به شرح زیر است:

۱. گره مبدأ که هیچ مسیری به مقصد ندارد فرآیند کشف مسیر را آغاز می‌کند. برای انجام این کار، پیام RREQ را انتشار می‌دهد و مقدار α _partial را برابر ۱ قرار می‌دهد.

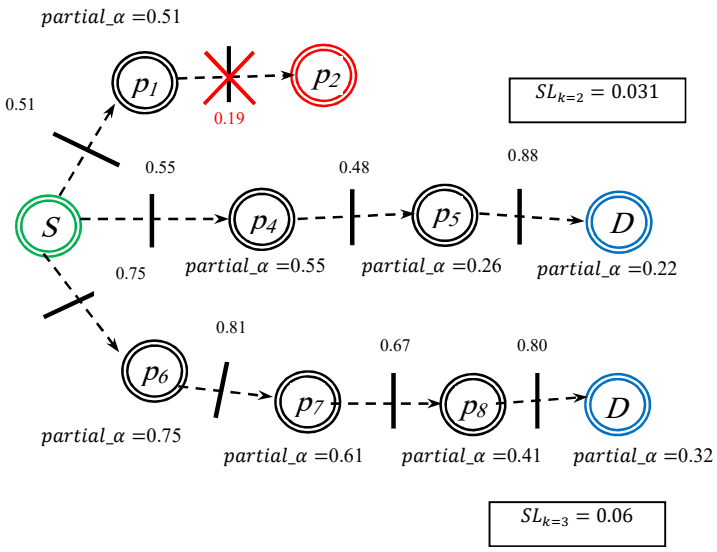
۲. هر گره میانی که پیام RREQ را دریافت کند تابع وارسی امنیت گره به گره را اجرا می‌کند. اگر مقدار α بیشتر از مقدار آستانه باشد با استفاده از معادله ۴-۵۸ مقدار α _partial را به‌روزرسانی می‌کند و تا زمانی که به مقصد برسد و یا گره‌ای مسیر تازه‌ای به آن داشته باشد این روند را ادامه می‌دهد.

۳. اگر یک گره میانی مسیر تازه‌ای به مقصد داشته باشد یک پیام RREP را به‌صورت Unicast بازگشت می‌دهد. سپس مقدار α _final در آخرین مقدار α _partial ضرب می‌شود تا مقدار SL گره میانی حاصل شود و اگر مقصد باشد آخرین مقدار α _partial به گره مبدأ بازگشت داده خواهد شد.

۴. با ارسال بازگشتی پیام RREP، تمام گره‌های میانی که هیچ مسیری به مقصد ندارند مدخلی با مقدار SL که با α _Final برابر است را اضافه می‌کنند. این امر زمانی درست است که گره‌های میانی مسیری با مقدار SL کمتر از α _Final داشته باشند. در این صورت این گره‌ها

مسیر قدیمی را با جدیدتر آن جایگزین می‌کنند. برای گره شروع‌کننده فرآیند نیز به همین صورت است.

نمونه‌ای از اجرای پروتکل FPN-SAODV در شکل ۴-۱۷ شبیه‌سازی شده است. ابتدا گره مبدأ S بسته RREQ را با مقدار partial_ α = 1 برای رسیدن به مقصد منتشر می‌کند. همان‌طور که در شکل نشان داده شده، به نظر می‌رسد سه مسیر مجزا منتهی به مقصد وجود دارد. با اجرای تابع وارسی امنیت گره به گره، مسیر k = 1 برای رسیدن به مقصد قطع می‌شود چراکه در این مسیر، گره مخرب P2 وجود دارد. برای مسیرهای K = 2 و k = 3 که تمام مسیرهای میانی آن‌ها با مقدار آستانه برآورده می‌شود مقدار SL_K برای آن‌ها محاسبه می‌شود و درنهایت، مسیری با بزرگ‌ترین مقدار SL_K (مسیر K = 3) انتخاب می‌شود. اگر در ابتدا (مسیر K = 2) به گره مبدأ برسد پس از آن تمام گره‌های میانی و همچنین گره سازنده به مسیری با مقدار SL بزرگ‌تر مواجه می‌شوند که جدول مسیریابی خود را با این مسیر امن‌تر جایگزین می‌کنند.



شکل ۴-۱۷. مثالی از نحوه کارکرد پروتکل اصلاحی مبتنی بر شبکه پتری فازی ارائه شده در یک شبکه فرضی با یک گره متخاصم

فصل ۵– پیاده‌سازی و ارزیابی

همان‌طور که قبلاً بیان شد در ارزیابی روش ارائه شده در تحلیل کارایی شبکه موردی سیار در مقابل حملات از روش ارزیابی مقایسه‌ای استفاده خواهد شد. به این صورت که مقادیر استخراج شده از مدل SRN ارائه شده برای هر لایه با مقادیر مستخرج از شبیه‌ساز NS-2 مقایسه می‌شود. تطابق مقادیر مستخرج از این دو محیط نشان‌دهنده صحت مدل ارائه شده برای هریک از لایه‌ها خواهد بود. به همین منظور با تعریف یک سناریو مشخص، ویژگی‌های آن را در شبیه‌ساز NS-2 تنظیم و همچنین مقادیر مستخرج از این ویژگی‌ها را در تنظیمات هریک از مدل‌های مربوط به لایه‌های پیوند داده و شبکه اعمال خواهد شد. پیاده‌سازی مدل‌های SRN ارائه شده در فصل قبل در نرم‌افزار SPNP [۶۹] انجام شده است. این نرم‌افزار دارای قابلیت کامل پیاده‌سازی مدل‌های SRN می‌باشد. همچنین تحلیل و ارزیابی یک مدل ارائه شده در این نرم‌افزار از طریق استخراج پارامترهای ارزیابی با استفاده از توابع تعریف شده صورت می‌گیرد. با توجه به نوسان مشاهده‌شده در نتایج به دست آمده از شبیه‌ساز NS-2 تصمیم به اجرای ۵ باره هر سناریو و میانگین‌گیری از نتایج به دست آمده به ازای هر معیار ارزیابی شده است. در شبیه‌سازی هریک از دو محیط از یک رایانه با پردازشگر Intel دوهسته‌ای با قدرت پردازشی ۲,۲ گیگاهرتز، حافظه RAM به ظرفیت ۴ گیگابایت و سیستم‌عامل Ubuntu نسخه ۸,۱۰ استفاده شده. همان‌طور که در بخش ۴-۱ مطرح شد با توجه به وابستگی مقادیر گذارهای موجود در مدل SRN لایه شبکه به معیارهای مستخرج از مدل SRN لایه پیوند داده مجبور به حل و ارزیابی لایه پیوند داده در ابتدا خواهیم بود. در ادامه، ابتدا در بخش ۵-۱ به توضیح سناریو پیاده‌سازی شده می‌پردازیم سپس به ترتیب در بخش‌های ۵-۲ و ۵-۳ حل مدل‌های مرتبط با پیوند داده و لایه شبکه و نتایج به دست آمده از آن تشریح خواهد شد. در بخش ۵-۴ نیز مدل مسیریابی امن مبتنی بر شبکه پتری فازی توضیح داده شده در بخش ۴-۳ مورد تحلیل و ارزیابی قرار خواهد گرفت.

۵-۱- تشریح سناریو استفاده شده

در یک سناریو مشخص تعدادی گره در یک شبکه با گنجایش ۲ مگابایت در یک فضای با ابعاد ۸۰۰ در ۸۰۰ متر با استفاده از پروتکل مسیریابی AODV و مدل حرکتی Random Way Point در حرکت هستند. گره‌ها با انتخاب یک نقطه مقصد به‌طور تصادفی با سرعتی که به‌طور یکنواخت[1] از محدوده $0(V_{min})$ تا $۲۰(V_{max})$ انتخاب می‌شود به سمت آن حرکت می‌کنند. مدت زمان توقف گره‌ها (τ_P) در مقصد برابر ۱۲۰ ثانیه تنظیم شده است. هر گره دارای شعاع انتقال ۱۵۰ متر و شعاع حساسیت گوش دادن ۲۵۰ متر می‌باشد.

۵-۲- ارزیابی لایه پیوند داده

به‌منظور ارزیابی صحت مدل ارائه شده برای پروتکل IEEE 802.11 DCF در این تحقیق از روش ارزیابی مقایسه‌ای استفاده شده است. به همین منظور صحت مدل ارائه شده به ازای معیار ارزیابی **زمان تأخیر یک گامه**[2] و **توان گذردهی لایه پیوند داده**[3] بررسی می‌شود. این معیارها با استخراج از مدل SRN لایه پیوند داده با نتایج به دست آمده از محیط NS-2 مقایسه خواهد شد. زمان تأخیر در اینجا متناظر با مدت زمانی است که طول می‌کشد یک گره به کانال دسترسی پیدا کند تا وقتی‌که از طرف گره مقصد در یک ارتباط یک گامه[4] بسته ACK را دریافت کند و یا آنکه بسته به علت رسیدن به حداکثر تعداد تلاش مجاز دور انداخته شده باشد. این معیار با استفاده از قانون Little بر اساس رابطه ۵-۱ از مدل برهم‌کنش گره‌ها به دست می‌آید.

$$\text{One hop Delay} = \frac{\mathrm{N}-\mathrm{m}(\mathrm{P_N})}{\mathrm{Thr}(\mathrm{T_{DS}})} \qquad (۱-۵)$$

---

[1] uniformly
[2] One hop communication Delay
[3] Throughput
[4] One hop communication

در این رابطه، $m(P_N)$ متناظر با متوسط تعداد نشانه در مکان P_N و $Thr(T_{DS})$ نیز متناظر با توان گذردهی گذار T_{DS} هست. $N - m(P_N)$ نیز به‌صورت مفهومی ناظر به تعداد بسته‌های داده‌ای است که در حال دریافت سرویس در سیستم هستند.

همچنین توان گذردهی نیز معرف تعداد بسته‌های داده‌ای است که به سلامت به گره مقصد خود در یک ارتباط یک گامه رسیده‌اند و درواقع پیغام ACK برای آن‌ها دریافت شده است. این معیار ارزیابی نیز با محاسبه توان گذردهی گذار T_{ACK} محاسبه خواهد شد (رابطه ۵-۲).

$$Throughput_D = Thr(T_{Ack}) \qquad (۲-۵)$$

۵-۲-۱-حل مدل‌های SRN لایه پیوند داده

برای حل دو مدل SRN ارائه شده لایه پیوند داده لازم است ابتدا مشخصه‌های مجهول هریک از دو مدل را به دست آوریم. بعد از تعیین زمان و یا نرخ اجرای گذارهای زمان‌دار و احتمال اجرای گذارهای آنی که در یک ساختار انتخاب از آن‌ها استفاده شده به تعیین مشخصه‌های مجهول موجود در دو مدل اقدام می‌کنیم. مشخصه‌های مجهول شامل نرخ فعالیت گذارهای T_{DR} و T_{DS} در مدل‌های جزئی و برهم‌کنش گره‌ها در لایه پیوند داده، تعداد نشانه‌های موجود در مکان‌های P_N و P_{N-m} در مدل برهم‌کنش گره‌ها و تعیین زمان و احتمال گذارهایی است که مبتنی بر مدل می‌باشند. در فصل ۵ راجع به نحوه استخراج آن‌ها توضیح داده شده است. با توجه به اینکه مشخصه‌های مجهول مبتنی بر مدل هم در مدل جزئی گره‌ها و هم در مدل برهم‌کنش گره‌ها وجود دارد مجبوریم که از روش تکرار از یک نقطه ثابت[1] [۷۰] برای حل آن استفاده شود. بر اساس این روش با انتساب یک مقدار اولیه به هریک از پارامترها از رویکرد حل تکراری[2] مدل‌ها تا زمان همگرا شدن یکی از پارامترهای

[1] Fixed point iteration
[2] Iterative

ارزیابی به یک مقدار با یک خطای کمینه استفاده خواهد شد. خلاصه مراحل کار برای حل مدل‌ها به‌صورت زیر می‌باشد:

۱. محاسبه تعداد نشانه‌های موجود در مکان‌های P_N و P_{N-m} تعداد گره‌های موجود در ناحیه مخفی با توجه به شرایط مسئله و با استفاده از روابط ۴-۲۲، ۴-۲۲ و ۴-۳۰
۲. تعیین زمان اجرای گذارها در مدل جزئی گره‌ها در دو حالت، برای گره‌های مشروع و گره‌های متخاصم و تخمین یک مقدار اولیه برای α و β.
۳. تعیین زمان اجرای گذارها در مدل برهم‌کنش گره‌ها برای دو جریان موجود جهت گره‌های مشروع و گره‌های متخاصم
۴. به‌روزرسانی مقادیر α، β، μ و δ بر اساس روابط ۴-۶، ۴-۸، ۴-۱۲، ۴-۱۴ و یا تخمین یک مقدار اولیه برای اولین بار
۵. اجرای مدل جزئی گره‌ها با استفاده از آخرین مقدار به دست آمده برای α و β.
۶. اجرای مدل برهم‌کنش گره‌ها با استفاده از آخرین مقدار به دست آمده برای μو δ.
۷. استخراج معیارهای ارزیابی از مدل برهم‌کنش گره‌ها با استفاده از روابط ۵-۱ و ۵-۲
۸. محاسبه خطای مقدار معیار و پرش به مرحله ۴ در صورت کوچک‌تر بودن از مقدار آستانه. در غیر این صورت اتمام فرآیند.

۵-۲-۲-پیاده‌سازی و نتایج لایه پیوند داده

برای ارزیابی هریک از معیارهای ارزیابی‌های توضیح داده شده در بخش ۵-۳ سناریو موردنظر با تعداد مختلف گره (از ۴۰ تا ۱۰۰) پیاده‌سازی شده است. فرض می‌شود که در هر سناریو ۲۰٪ تعداد گره‌های آن به‌عنوان گره متخاصم عمل کنند که هرکدام با یکی از روش‌های حمله در لایه پیوند داده مطابق با توضیحات موجود در بخش ۴-۱-۶ عمل می‌کنند. نرخ CBR در شبیه‌ساز NS-2 و توان گذردهی در لایه شبکه (بر اساس رابطه ۵-۴) به نحوی تنظیم شده‌اند که ترافیک داده ارسالی به لایه

پیوند داده برابر با سه نرخ متفاوت به اندازه ۳۰۰ کیلوبایت بر ثانیه، ۶۰۰ کیلوبایت بر ثانیه و ۱ مگابایت بر ثانیه باشد. شکل‌های ۵-۱ تا ۵-۳ نتایج به دست آمده را به ازای هریک از معیارهای ارزیابی نشان می‌دهد. هر شکل از دو قسمت الف و ب تشکیل شده است که به ترتیب نشان‌دهنده مقدار معیارهای ارزیابی توان گذردهی لایه انتقال و تأخیر می‌باشند. در هر شکل خطوط پر نشان‌دهنده مقادیر به دست آمده از مدل SRN ارائه شده می‌باشد. درعین‌حال خطوط نقطه‌چین نیز معرف مقادیر به دست آمده از شبیه‌ساز NS-2 است. به‌طورکلی همان‌طور که از نتایج برمی‌آید صرف‌نظر از تفاوت قابل‌چشم‌پوشی که در نتایج مشاهده می‌شود مقادیر به دست آمده از مدل SRN ارائه شده با مقادیر به دست آمده از NS-2 کاملاً منطبق و دارای یک رویکرد می‌باشد. همان‌طور که از شکل‌ها برمی‌آید با افزایش تعداد گره‌های شبکه، مقدار توان گذردهی گره‌ها کاهش خواهد یافت. این روند هم در یک شبکه امن بدون هیچ گره متخاصم و هم در شبکه‌ای که در آن گره‌های متخاصم در کنار گره‌های مشروع در حال ارسال داده هستند صادق است. این مورد می‌تواند به‌این‌علت باشد که با افزایش تعداد کل گره‌های موجود در یک شبکه تعداد گره‌های واقع در یک همسایگی افزایش یافته که این امر سبب افزایش احتمال ایجاد برخورد در ارسال داده‌ها و کاهش مقدار نرخ توان گذردهی خواهد شد. در مدل ارائه شده تعداد گره‌های موجود در یک همسایگی توسط رابطه ۴-۲۲ به دست می‌آید و مقدار آن در مکان P_N از مدل برهم‌کنش گره‌ها تنظیم می‌شود که افزایش آن سبب افزایش مقدار متوسط نشانه در مکان $P_{Backoff}$ و درنهایت افزایش احتمال اجرای گذار T_{nsent} بر اساس رابطه ۴-۱۲ خواهد شد.

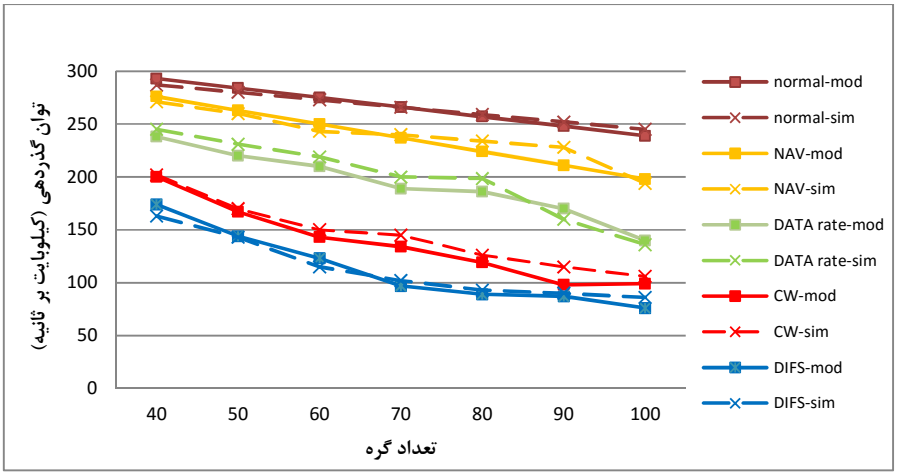
در ارتباط با معیار توان نرخ توان گذردهی به نظر می‌رسد که حملات دست‌کاری پنجره انتظار تعویق و بازه انتظار DIFS دارای تأثیر بیشتری نسبت به سایر حملات هستند و به ازای این حملات شاهد کاهش بیشتری در این معیار هستیم. بیشترین تأثیر منفی از افزایش تعداد گره‌های شبکه را به ازای حمله دست‌کاری پنجره انتظار تعویق شاهد هستیم. همچنین کمترین میزان نرخ توان گذردهی را به ازای حمله دست‌کاری بازه انتظار DIFS شاهد هستیم. مقدار نرخ توان گذردهی در این نوع از حمله

در بدترین شرایط به ۱۰۰، ۲۵۰ و ۴۰۰ مگابایت برثانیه رسیده است، که به ترتیب برای نرخ‌های ارسال داده ۳۰۰ کیلوبایت بر ثانیه، ۷۰۰ کیلوبایت بر ثانیه و ۱ مگابایت بر ثانیه می‌باشد.

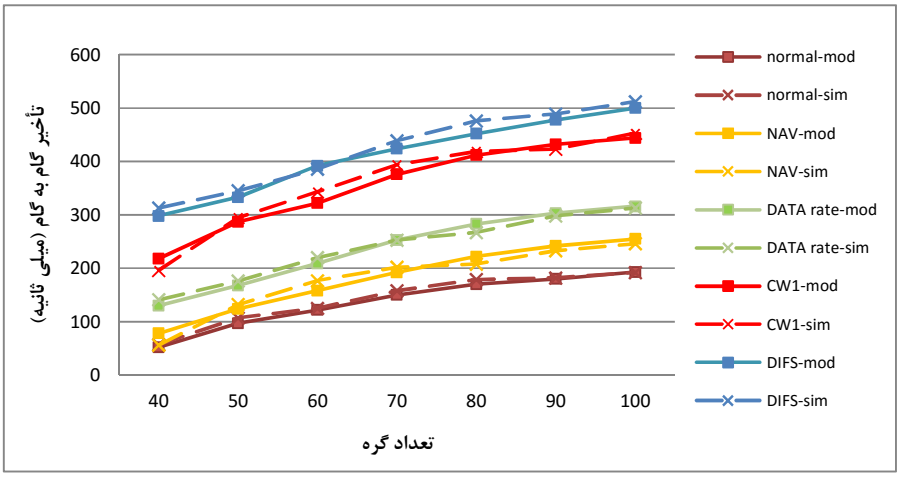
در ضمن همان‌طور که از شکل‌ها برمی‌آید به نظر می‌رسد حمله دست‌کاری طول پنجره NAV کمترین تأثیر را در نرخ گذردهی شبکه داشته است بطوریکه در بسیاری از موارد مقدار به دست آمده برای معیار نرخ توان گذردهی با مقدار به دست آمده به ازای یک شبکه امن بدون گره متخاصم یکسان است. در بدترین شرایط در این حمله میزان نرخ توان گذردهی به اندازه ۲۰٪ کاهش خواهد یافت. علتی که می‌توان برای توجیه روند برای این حمله می‌توان ارائه داد این است که گره صاحب کانال بعد اتمام موفقیت‌آمیز هریک از مراحل پروتکل دست تکانی RTS/CTS تنها به اندازه یک بازه زمانی SIFS صبر می‌کند که مقدار آن کمتر از طول بازه زمانی یک برش است. از طرفی گره متخاصم که قصد تداخل در ارسال سیگنال داده توسط گره جاری و تصاحب کانال را دارد باید ارسال خود را در ابتدای یک برش زمانی انجام دهد که طول آن بیشتر از یک SIFS است. بنابراین در انجام عمل خود ناتوان خواهد شد. تأثیر حمله دست‌کاری در نرخ ارسال داده نیز در میانه حملات دیگر لایه انتقال قرار می‌گیرد. به‌طور میانگین به ازای اعمال این حمله ۳۰٪ از نرخ توان گذردهی گره‌ها کاسته خواهد شد.

مقدار معیار تأخیر ارسال داده در مقابل افزایش تعداد گره‌های شبکه رویکردی متفاوت با آنچه برای معیار نرخ توان گذردهی است، دارد. همان‌طور که در شکل‌های ۵-۱ (ب)، ۵-۲ (ب) و ۵-۳ (ب) نشان داده شده با افزایش تعداد گره‌ها، تأخیر بیشتری در ارسال داده تا رسیدن به مقصدشان در یک ارتباط یک گامه شاهد هستیم. همچنین با افزایش نرخ ارسال داده نیز میزان این معیار افزایش می‌یابد. در بدترین شرایط حداکثر زمان تأخیر به دست آمده در اجرای حمله دست‌کاری بازه انتظار DIFS رخ داده در حالتی که نرخ ارسال داده برابر ۱ مگابایت بر ثانیه باشد که در این حالت مقدار این معیار برابر ۶۰۰ میلی‌ثانیه است. در مقابل حمله دست‌کاری تایمر NAV کمترین تأثیر را روی این معیار داشته است. در بسیاری از موارد نتیجه به دست آمده از آن با یک شبکه نرمال که در آن گره متخاصمی

وجود ندارد یکسان است و البته حمله دست‌کاری در سرعت ارسال داده نیز تا حدوی مانند حمله NAV می‌باشد. در بدترین شرایط به ازای نرخ ارسال داده ۱ مگابایت بر ثانیه، تأخیری برابر با ۳۸۰ میلی‌ثانیه را در ارسال بسته‌ها شاهد هستیم. همانند معیار نرخ توان گذردهی، در معیار تأخیر ارسال داده نیز حملات دست‌کاری بازه DIFS و پنجره تعویق بیشترین تأثیر منفی را در عملکرد شبکه داشته‌اند که در حالتی به زمان تأخیر ۶۰۰ میلی‌ثانیه هم رسیده است.

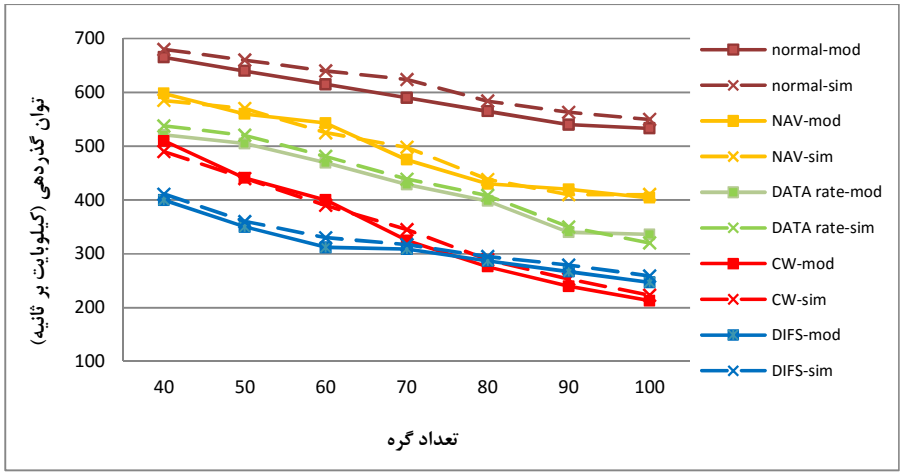


(الف)

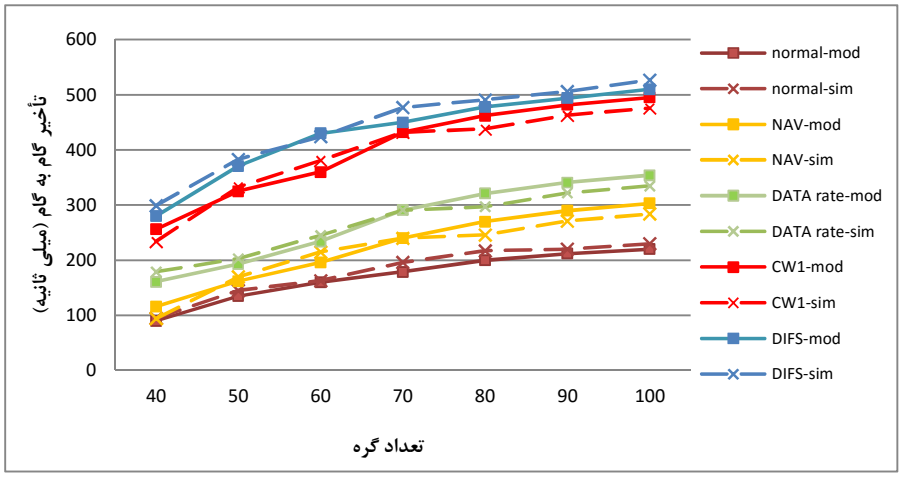


(ب)

شکل ۵-۱ نتایج به دست آمده به ازای معیارهای الف) توان گذردهی ب) تأخیر گام‌به‌گام برای ارزیابی پروتکل IEEE 802.11 DCF در مقابل اعمال چهار استراتژی حمله در لایه پیوند داده. با تنظیم نرخ تولید داده به مقدار ۳۰۰ کیلوبایت بر ثانیه

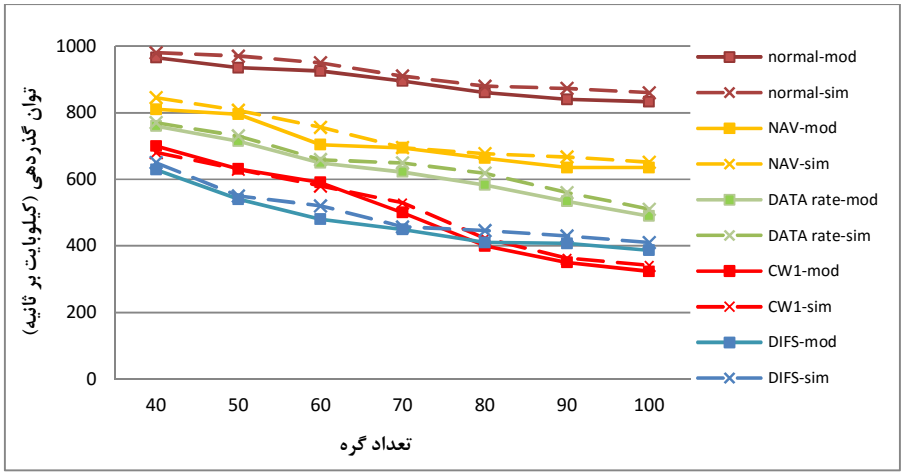


(الف)

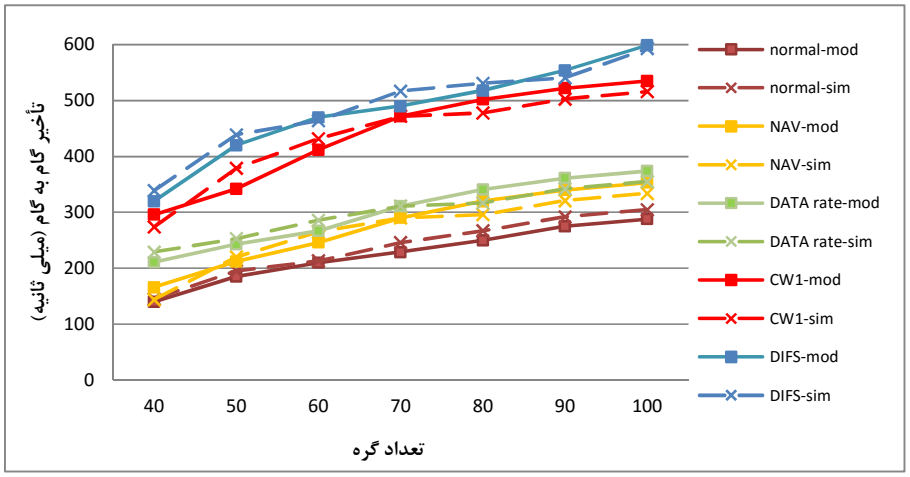


(ب)

شکل ۵-۲ نتایج به دست آمده به ازای معیارهای الف) توان گذردهی ب) تأخیر گام‌به‌گام برای ارزیابی پروتکل IEEE 802.11 DCF در مقابل اعمال چهار استراتژی حمله در لایه پیوند داده. با تنظیم نرخ تولید داده به مقدار ۷۰۰ کیلوبایت بر ثانیه



(الف)



(ب)

شکل ۵-۳ نتایج به دست آمده به ازای معیارهای الف) توان گذردهی ب) تأخیر گام‌به‌گام برای ارزیابی پروتکل IEEE 802.11 DCF در مقابل اعمال چهار استراتژی حمله در لایه پیوند داده. با تنظیم نرخ تولید داده به مقدار ۱ مگابایت بر ثانیه

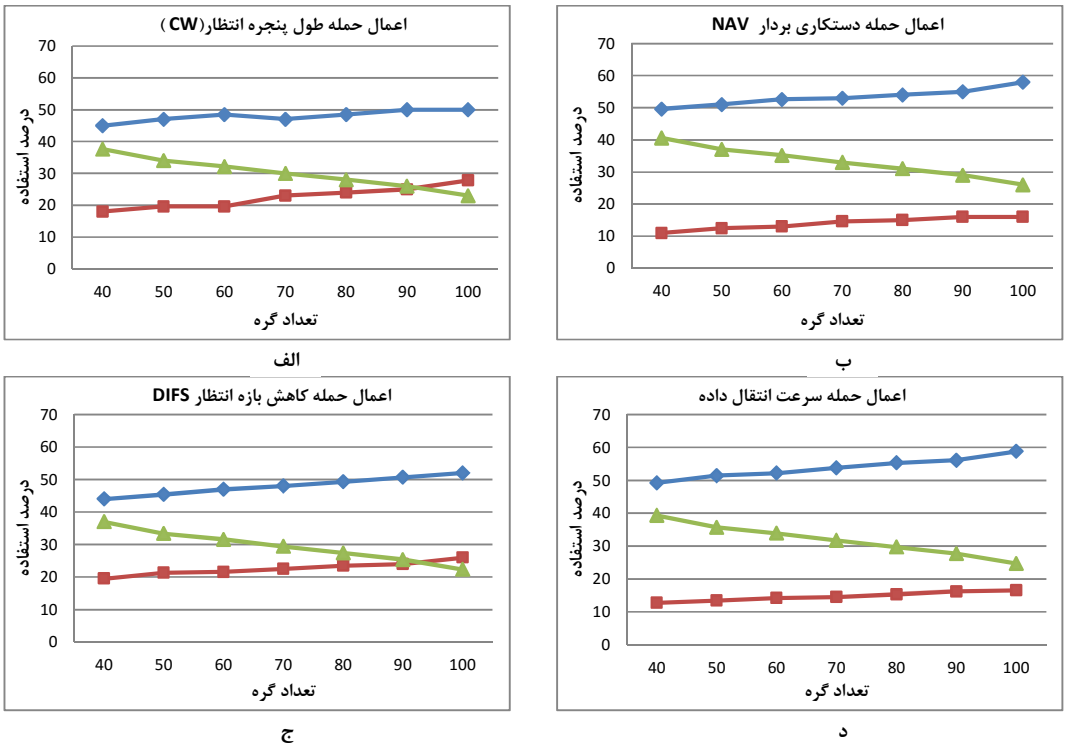
با اطمینان از صحت مدل ارائه شده می‌توانیم به بررسی بیشتری در عملکرد پروتکل IEEE 802.11 DCF با تکیه بر مدل ارائه شده بپردازیم. لذا در تلاشی دیگر سه معیار ارزیابی درصد استفاده از کانال توسط گره‌های مشروع جهت ارسال داده، درصد استفاده از کانال توسط گره‌های متخاصم جهت ارسال داده و همچنین درصد آزاد بودن کانال بررسی و محاسبه شده است. مورد آخر ناظر بر حالتی است که در آن هیچ گره‌ای در حال ارسال داده نیست و یا آن‌که مشغول گذراندن بازه انتظار اولیه و یا انتظار

تعویق می‌باشند. هریک از این سه معیار توسط روابط ۵-۳ تا ۵-۴ محاسبه می‌شوند. همچنین نتایج بدست آمده از این معیارها در شکل های ۵-۴ تا ۵-۶ نشان داده شده است. در کلیه موارد خطوط آبی و قرمز به ترتیب نشان دهنده نتایج بدست آمده برای گره های مشروع و متخاصم می باشد. همچنین خطوط سبز رنگ نیز درصد بیکاری کانال را نشان می دهد.

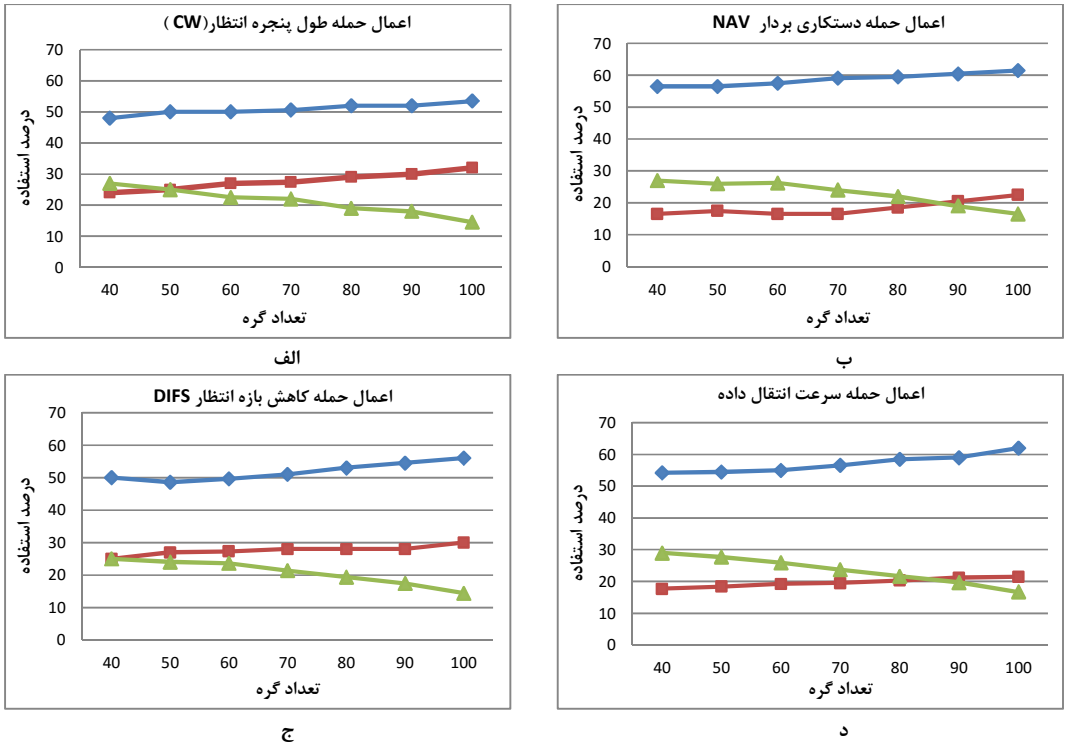
درصد استفاده از کانال توسط گره‌های مشروع جهت ارسال داده $= Pr((\neq P_{CTS} > 0)\ or\ ((\neq P_{RTS} > 0))\ or((\neq P_{DATA} > 0))\ or((\neq P_{ACK} > 0))\ or((\neq P_{timeout} > 0))$ (۵-۳)

درصد استفاده از کانال توسط گره‌های متخاصم جهت ارسال داده $= Pr((\neq P_{CTS-m} > 0)\ or\ ((\neq P_{RTS-m} > 0))\ or((\neq P_{DATA-} > 0))\ or((\neq P_{ACK-m} > 0))\ or((\neq P_{timeout-m} > 0))$ (۵-۴)

درصد آزاد بودن کانال $= Pr((\neq P_{ch} = 1)$ (۵-۵)

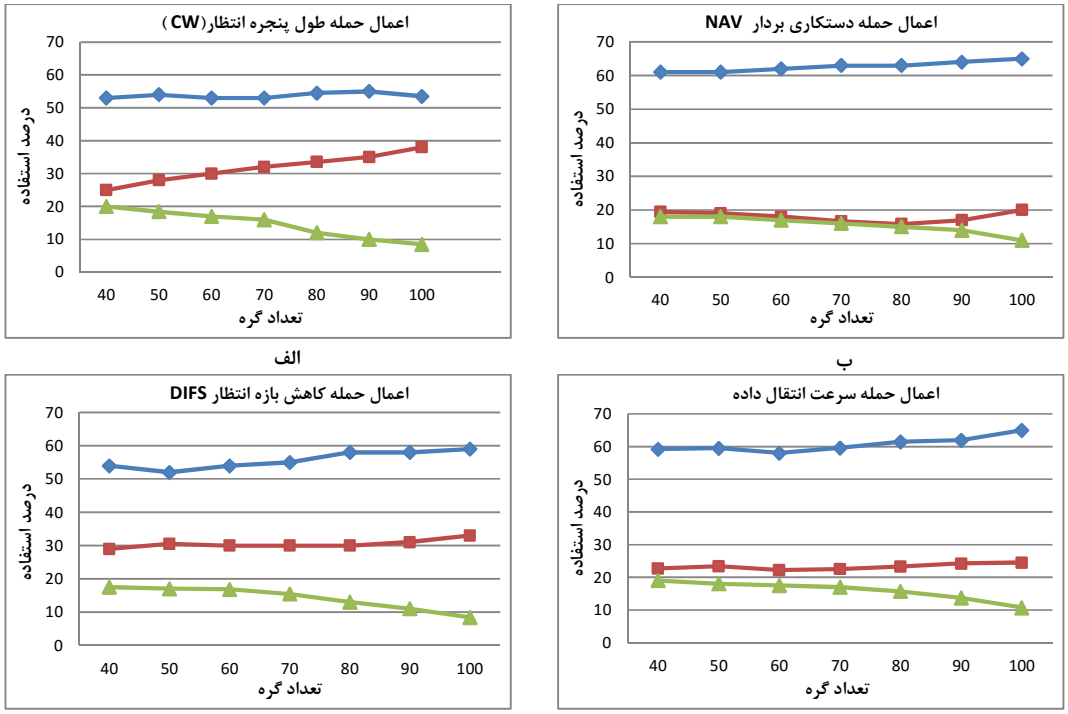


شکل ۵-۴ درصد استفاده از کانال برای گره‌های مشروع و متخاصم و درصد آزاد بودن برای حملات مختلف لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۳۰۰ کیلوبایت بر ثانیه. — مشروع، — متخاصم، — آزاد



شکل ۵-۵ درصد استفاده از کانال برای گره‌های مشروع و متخاصم و درصد آزاد بودن برای حملات مختلف لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۶۰۰ کیلوبایت بر ثانیه. — مشروع، — متخاصم، — آزاد

در ارزیابی صورت گرفته برای معیارهای توصیف‌شده توسط روابط ۵-۳ تا ۵-۵ هم مشخص شده که حملات کاهش بازه انتظار DIFS و دست‌کاری پنجره انتظار تعویق (CW) نسبت به حملات دیگر دارای اثر بیشتری بوده و گره‌های متخاصم با این نوع حمله با شانس بیشتری می‌توانند کانال را در اختیار بگیرند. همچنین در اینجا نیز مشاهده می‌شود که با افزایش تعداد گره‌ها و نرخ تولید بسته حمله دست‌کاری پنجره انتظار تعویق (CW) از کارکرد بیشتری برخوردار خواهد بود. این مورد برای حمله دست‌کاری بازه انتظار DIFS با افزایش تعداد گره‌ها درست نیست و در این مورد روند ثابتی را از گره‌های متخاصم شاهد هستیم. از موارد دیگری که از نتایج به دست آمده در شکل‌های ۵-۴ تا ۵-۶ استنباط می‌شود کاهش درصد بیکاری کانال با افزایش تعداد گره‌ها و نرخ تولید داده می‌باشد.

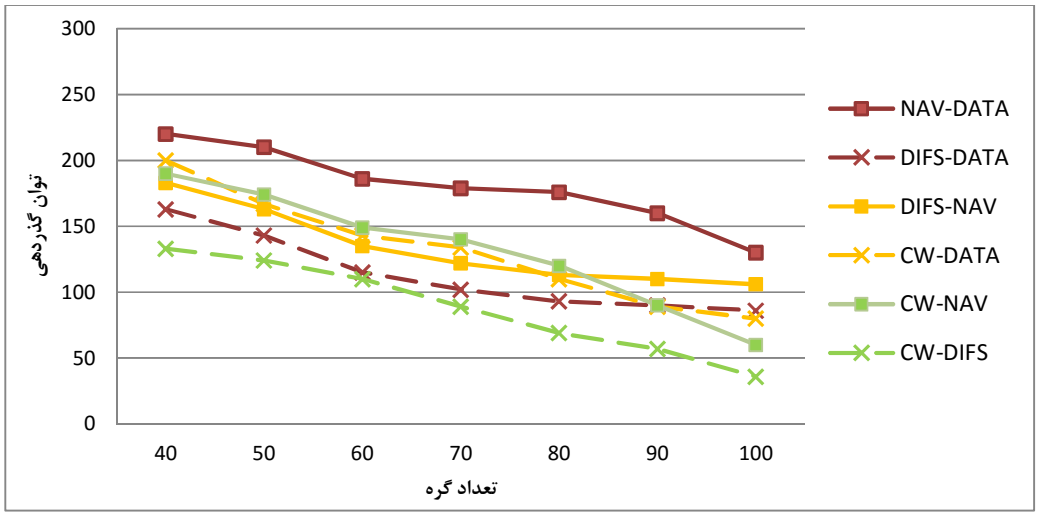


شکل ۵-۶ درصد استفاده از کانال برای گره‌های مشروع و متخاصم و درصد آزاد بودن برای حملات مختلف لایه پیوند داده. با تنظیم نرخ تولید بسته به مقدار ۱ مگابایت بر ثانیه. — مشروع، — متخاصم، — آزاد

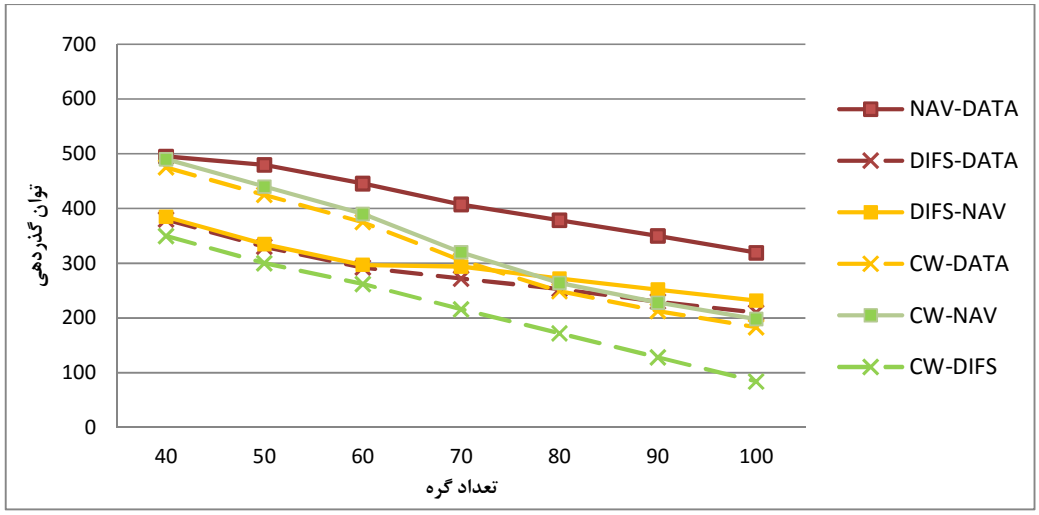
در کلیه آزمایش‌ها جمع درصد به‌کارگیری کانال توسط گره‌های متخاصم و مشروع و همچنین بیکاری کانال برابر ۱۰۰ بوده که نشان‌دهنده درستی مدل ارائه شده می‌باشد. همچنین در بررسی دیگری در ارتباط با صحت مدل، احتمال حضور دو نشانه و یا بیشتر در مکان $P_{channel}$ توسط نرم‌افزار اندازه‌گیری شده که برابر صفر بوده است.

بمنظور ارزیابی دقیق‌تر اثر حملات لایه پیوند داده بر عملکرد پروتکل IEEE 802.11 DCF در ادامه به مطالعه اثر اعمال متداخل و همزمان حملات در این لایه با استفاده از مدل ارائه شده می‌پردازیم. با در نظر گرفتن چهار حمله بررسی شده به شش حمله ترکیبی خواهیم رسید. این حملات شامل موارد حمله توأمان دستکاری مکانیزم انتظار تعویق (CW) و بازه انتظار DIFS ، حمله توأمان دستکاری مکانیزم انتظار تعویق (CW) و تایمر NAV، حمله توأمان دستکاری مکانیزم انتظار تعویق (CW) و سرعت انتقال داده (DATA)، حمله توأمان دستکاری بازه انتظار اولیه (DIFS) و تایمر NAV، حمله توأمان دستکاری بازه انتظار اولیه (DIFS) و سرعت انتقال داده (DATA)، حمله توأمان دستکاری

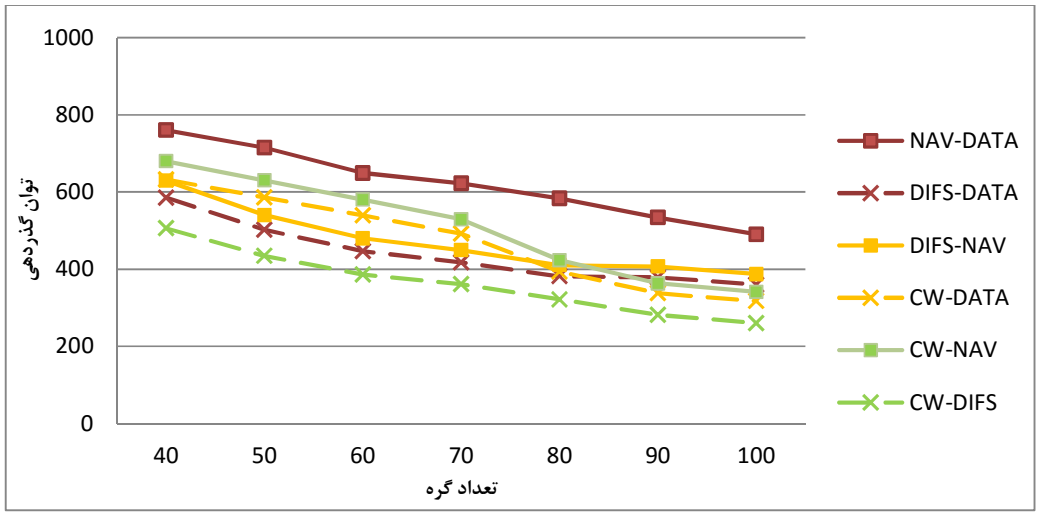
تایمر NAV و سرعت انتقال داده (DATA). شکل‌های ۵-۷ تا ۵-۹ به ترتیب نتایج شش ترکیب حمله فوق به ازای نرخ‌های ارسال داده ۳۰۰ کیلوبایت بر ثانیه، ۷۰۰ کیلوبایت بر ثانیه و یک مگابایت بر ثانیه را نشان می دهد. همانطور که از شکل‌ها بر می‌آید حمله ترکیبی دستکاری پنجره انتظار تعویق و کاهش بازه انتظار اولیه DIFS دارای اثر مخرب بیشتری بر عملکرد شبکه است. با توجه به تعداد محدود گره های متخاصم و نرخ ثابت تولید داده توسط آن‌ها براساس آنچه که از تنایج مشخص شده است اینطور نبوده که به اندازه مجموع جداگانه اثر حملات از مقدار توان گذردهی گره‌های مشروع کاسته شود. در اینجا هم مشخص شده که حملات ترکیبی که شاکل حمله دستکاری مکانیزم انتظار تعویق باشند، با افزایش تعداد گره‌ها و نرخ تولید داده به مقدار بیشتری از توان گذردهی گره‌های مشروع می‌کاهند. همچنین حمله ترکیبی دستکاره تایمر NAV و سرعت انتقال داده کمترین میزان تأثیر در توان گذردهی گره‌های مشروع را داشته است.



شکل ۵-۷ نتایج به دست آمده از اعمال حملات ترکیبی در لایه پیوند داده برای معیار توان گذردهی با تنظیم نرخ تولید داده به مقدار ۳۰۰ کیلوبایت بر ثانیه



شکل ۵-۸ نتایج به دست آمده از اعمال حملات ترکیبی در لایه پیوند داده برای معیار توان گذردهی با تنظیم نرخ تولید داده به مقدار ۷۰۰ کیلوبایت بر ثانیه



شکل ۵-۹ نتایج به دست آمده از اعمال حملات ترکیبی در لایه پیوند داده برای معیار توان گذردهی با تنظیم نرخ تولید داده به مقدار ۱ مگابایت بر ثانیه

۵-۲-۳-ارزیابی پیچیدگی زمانی جهت استخراج معیارهای کارایی

همانطور که گفته شد یکی از دلایل ارائه مدل پتری برای ارزیابی شبکه‌های موردی سیار در این تحقیق کاهش زمان اجرا در مقابل پیاده‌سازی آن در شبیه‌سازهایی مانند NS-2 می‌باشد. لذا در این بخش به بررسی رابطه زمانی اجرای سناریو در محیط شبیه‌ساز NS-2 و اجرای مدل SRN ارائه شده در SPNP پرداخته خواهد شد. به‌طورکلی، حل یک مدل SRN به‌طور فزآینده‌ای به تعداد حالت‌های ایجاد شده از مدل مارکوف معادل و قدرت پردازش ماشین استفاده شده وابسته است. تعداد حالت‌های ایجاد شده در مدل مارکوف مستخرج از مدل برهم‌کنش گره‌ها به تعداد نشانه‌های موجود در مکان‌های P_N و P_{N-m} که متناظر با تعداد گره‌های مشروع (N) و متخاصم (N_m) موجود در یک همسایگی می‌باشد وابسته است. در مدل SRN مربوط به عملکرد جزئی گره‌ها نیز این وابستگی به مقدار MRL و طول پنجره انتظار تعویق وجود دارد. بیشترین تعداد حالت‌های ایجاد شده در مدل مارکوف ایجاد شده از مدل SRN رفتار جزئی گره‌ها و برهم‌کنش گره‌ها به ترتیب برابر ۴۵۳۰ و ۴۳۸۵ بوده است. البته این مورد تأثیر زیادی روی زمان اجرای لازم جهت برآورد معیارهای ارزیابی نداشته است و در بدترین شرایط این مقدار به کمتر از ۴۰ ثانیه رسیده است. از طرف دیگر زمان سپری‌شده جهت اجرای سناریو در محیط شبیه‌ساز NS-2 نیز به‌شدت به تعداد گره‌های متخاصم و مشروع وابسته بوده و نسبت به افزایش آن ارتباط نمایی دارد. در بعضی از موارد زمان سپری‌شده جهت استخراج یک معیار ارزیابی به ازای یک بار اجرای شبیه ساز به مدت ۷۵ دقیقه به طول انجامیده که با فرض ۵ تا ۷ بار اجرای یک سناریو .و میانگین‌گیری از نتایج کل زمان لازم جهت استخراج نتایج از شبیه ساز ۴-۷ ساعت شده است. در جدول ۵-۱ زمان لازم جهت استخراج نتایج معیارهای ارزیابی کارایی از مدل ارائه شده و شبیه ساز NS-2 نشان داده شده است. زمان محاسبه شده برای استخراج نتایج از شبیه ساز NS-2 تنها شامل زمان یک بار اجرا تا تولید فایل trace بعلاوه زمان لازم جهت اعمال کد awk روی فایل trace اعمال شده است.

جدول ۵-۱ نتایج مربوطه به پیچیدگی زمانی اجرای مربوط به محیط شبیه ساز NS-2 و استخراج نتایج از مدل

زمان لازم جهت استخراج نتایج از شبیه ساز	زمان لازم جهت استخراج نتایج از مدل	تعداد گره
۹ دقیقه	۸ ثانیه	۴۰
۱۲ دقیقه	۸ ثانیه	۵۰
۲۴ دقیقه	۱۰ ثانیه	۶۰
۳۲ دقیقه	۱۸ ثانیه	۷۰
۴۰ دقیقه	۲۶ ثانیه	۸۰
۱ ساعت و ۲ دقیقه	۳۱ ثانیه	۹۰
۱ ساعت و ۱۵ دقیقه	۳۹ ثانیه	۱۰۰

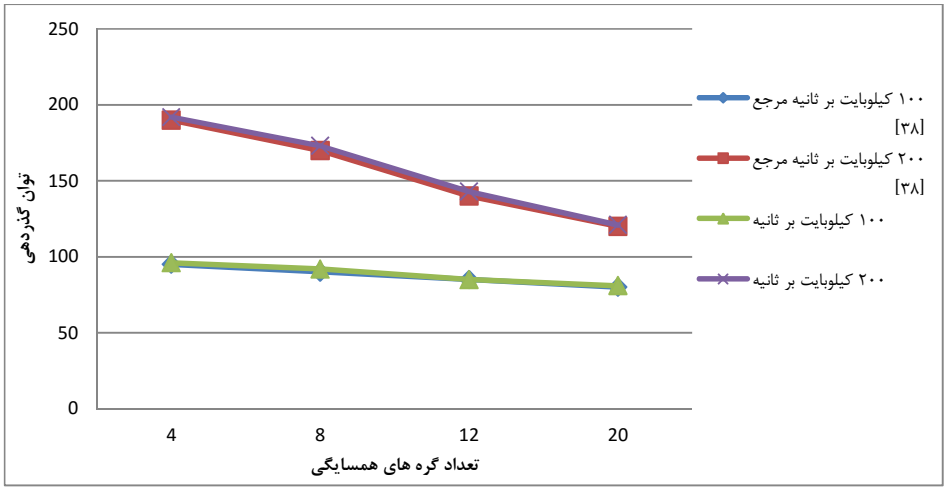
۵-۲-۴-ارزیابی مقایسه ای با کارهای پیشین

هرچند که در اثبات صحت هر یک از نتایج بدست آمده از روش ارزیابی مقایسه‌ای استفاده شده است، در این قسمت بر آن شده‌ایم تا نتایج کار خود را با پژوهش‌های پیشین انجام شده در این زمینه مقایسه کنیم. مساله اصلی در انجام این مقایسه، تفاوت بعضاً عمده مطالعات پیشین در مدل‌سازی پروتکل‌های لایه پیوند داده با مطالعه انجام شده توسط این تحقیق می‌باشد. تفاوت‌های موجود عمدتاً شامل مسائلی مانند عدم توجه به مسئله گره مخفی، مکانیزم دست تکانی RTS/CTS، حرکت پویای گره‌ها و یا مسأله گره‌های متخاصم بوده است. با این وجود، در بخش حاضر سعی شده است با انتخاب چند مطالعه شاخص که نزدیکی بیشتری با تحقیق حاضر داشته‌اند به این مقایسه پرداخته شود. در انجام هر آزمایش، محیط شبیه سازی یک مطالعه پیشین مبنا قرار گرفته و با نگاشت مقادیر آن در مدل ارائه شده در این تحقیق، از نتایج آن استفاده شده است. همانطور که در بخش ۳-۱ توضیح داده شده است هه و همکاران[1] در [۳۸] کارایی الگوریتم IEEE 802.11 DCF را در یک شبکه چندگامه با ارائه یک مدل تحلیلی بررسی نمودند. مدل ارائه شده مبتنی بر یک زنجیره مارکوف دو-بعدی جهت نشان دادن رفتار مکانیزم انتظار تعویق در این الگوریتم می‌باشد. در زنجیره مارکوف ارائه شده تأثیر

[1] He et al

مسئله گره مخفی در آن بررسی شده است. به‌منظور راحتی تحلیل در این تحقیق فرض است که گره‌ها در یک شبکه به‌صورت ثابت تحت توپولوژی مشبک[1] پراکنده شده‌اند. هرچند که مدل ارائه شده در مرجع [۳۸] تنها به مدل سازی مکانیزم backoff در پروتکل DCF پرداخته شده اما تأثیر مکتانیزم هایی مانند دست تکانی RTS/CTS و بازه انتظار اولیه DIFS و SIFS با استفاده از روابط ریاضی بعد از اجرای مدل به آن اضافه شده. است. همچنین تأثیر مساله گره مخفی در این تحقیق با استفاده از مدل های ریاضی در مدل گنجانده شده است. چنانچه که در صفحات ۸۹-۹۰ این تحقیق هم مشاهده می شود، مقدار احتمال گذارهای Tsent و Tnsent هم از روابط ریاضی موجود در این تحقیق (مرجع [۳۸]) بدست آمده است. در این تحقیق هیچ فرضی برای مدل سازی و بررسی حملات انجام نشده است. بنابرای کلیه نتایج آن با فرض عملکرد نرمال شبکه می باشد. بنابراین در مقایسه انجام شده با نتایج تحقیق ما نیز تعداد گره های متخاصم در مدل برهم کنش گره ها صفر فرض شده است و کلیه عملکرد های مربوط گره های متخاصم از مدل حذف شده یا صفر در نظر گرفته شده است. بعنوان تفاوتی دیگر، تعداد گره‌های موجود در یک فضای همسایگی در مرجع [۳۸] ثابت می‌باشد. بنابرای از ماژول محاسبه پویای تعداد گره ها در مدل خودمان نیز صرف نظر کرده ایم. همچنین آزمایشات انجام شده در این تحقیق با فرض کوچک بودن فضای حرکت گره‌ها و نرخ ترافیک بالای داده ارسالی محاسبه شده است که این به منظور نشان دادن تأثیر عامل گره مخفی (هدف اصلی این مقاله) می‌باشد. در مقایسه انجام شده توسط ما ترجیح داده شده است تا آزمایشاتی را از آن تحقیق در نظر بگیریم که عمومیت بیشتری (از نظر نرخ ارسال داده) در شبکه های موردی سیار داشته باشند.

[1] Grid



شکل ۵-۱۰ : مقایسه مقادیر بدست آمده برای معیار توان گذردهی از مرجع [۳۸] و مدل ارائه شده در این تحقیق

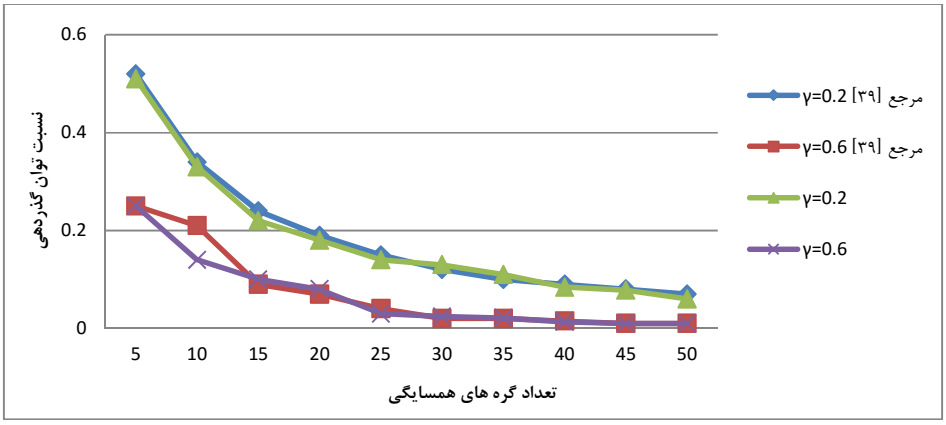
شکل ۵-۱۰ نتایج بدست آمده از مقایسه با مرجع [۳۸] را نشان می‌دهد. نتایج بدست آمده با فرض تولید داده توسط هر گره با نرخ ۲۰۰ کیلوبایت بر ثانیه و وجود ۴، ۸، ۱۲ و ۲۰ گره در یک همسایگی با محاسبه مقدار متوسط نرخ توان گذردهی نشان داده شده است. طول هر بسته مطابق با آنچه در این تحقیق ذکر شده بود برابر ۱ کیلوبایت در نظر گرفته شده است. مابقی پارامترهای لایه فیزیکی با آنچه که در تحقیق ما ارائه شده، یکسان بوده است.

همانطور که از شکل برمی‌آید نتایج بدست آمده از تحقیق کاملاً بر هم منطبق می باشند. هرچند که محیط تعریف شده برای آزمایش در مرجع [۳۸] با در نظر گرفتن تعداد گره های همسایگی و ابعاد شبکه پر تراکم می باشد اما ظاهراً نرخ ارسال داده ۱۰۰ کیلوبایت بر ثانیه مقدار بالایی نمی باشد. بنابراین افزایش تعداد گره های همسایگی تأثیر چندانی بر مقدار توان گذردهی گره‌ها نخواهد داشت و با افزایش آن مقدار آن (توان گذردهی) کاهش قابل ملاحظه‌ای نخواهد کرد. با افزایش نرخ توان گذردهی به ۲۰۰ کیلوبایت برثانیه تعداد گره‌های موجود در یک همسایگی تأثیر بیشتری بر عملکرد پروتکل داشته و مقدار توان گذردهی کاهش تقریباً قابل ملاحظه ای خواهد کرد.

به عنوان تنها کار شاخص که در مدل سازی حملات لایه پیوند داده انجام شد به مقایسه مقادیر استخراج شده از این تحقیق با تحقیق انجام شده در مرجع [۳۹] شده است. همانطور که در بخش ۳-

۱ مطرح شد نویسندگان این مقاله اقدام به ارائه یک مدل مارکوف سه-بعدی جهت مطالعه رفتار شبکه در اثر حملات لایه پیوند داده بر مبنای مرجع [۳۸] نموده اند. تنها حمله‌ای که در این تحقیق مورد مطالعه قرار گرفته است حمله کاهش پنجره انتظار تعویق می‌باشد. حمله اعمال شده به این صورت عمل می‌کند که در آن گره‌های متخاصم اقدام به کاهش طول پنجره انتظار تعویق به اندازه ضریب γ خواهند نمود. محیط شبیه سازی یک مربع ۱۰۰متر در ۱۰۰ متر فرض شده است و نتایج براساس نسبت توان گذردهی برای گره‌های متخاصم براساس تعداد گره‌های موجود در این فضا محاسبه شده است. برای همین منظور برای محاسبه این مقدار در رابطه ۵-۲ بجای $Thr(T_{Ack})$ از $Thr(T_{Ack-m})$ استفاده خواهد شد و نسبت آن به مجموع $Thr(T_{Ack})$ و $Thr(T_{Ack-m})$ بدست خواهد آمد. با توجه به اینکه هدف اصلی مرجع [۳۹] بررسی تنها حمله کاهش اندازه طول پنجره انتظار تعویق و بهبود آن بوده، بسیاری از آزمایشات آن مربوط به الگوریتم بهبودیافته ارائه شده و یا الگوریتم دست تکانی پایه BAبود که از میان آنها آزمایشی که قابل نگاشت با تحقیق صورت گرفته توسط ما بود انتخاب شد. نتایج به ازای تعداد گره های موجود در یک فضای همسایگی از ۵ تا ۵۰ بدست آمده است. براساس آزمایشات صورت گرفته در این مرجع، گره های متخاصم در اینجا می توانند اندازه پنجره انتظار تعویق را با ضریب ۰/۲ و ۰/۶ طول پنجره اصلی کوتاه نمایند. در اینجا نیز نشان داده شده است که نتایج بدست آمده از مدل ارائه شده در این تحقیق با مرجع [۳۹] یکسان می باشد که نشان دهنده صحت مدل ارائه شده توسط این تحقیق است. همانطور که از نتایج برمی‌آید با کاهش ضریب کوتاه کردن پنجره انتظار تعویق قدرت گره های متخاصم بیشتر شده و نسبت توان گذردهی این گره ها به گره های مشروع بیشتر خواهد شد. با فرض وجود ۵ گره در یک فضای همسایگی این نسبت از حدود ۰/۵ به ۰/۲۲ رسیده است. افزایش تعداد گره های موجود در همسایگی نیز براساس آنچه که انتظار می رفت سبب کاهش نسبت توان گذردهی برای گره متخاصم شده است. آنطور که از نتایج بر می آید وجود حدود ۲۰ همسایگی در فضای تعریف شده برای گره ها حد آستانه ای برای آن محسوب می

شود. با افزایش تعداد گره‌های همسایگی از این حد پروتکل DCF قادر به گذردهی حجم داده ارسالی توسط گره ها را نخواهد داشت و نسبت توان گذردهی بطور قابل ملاحظه ای کاهش می‌یابد.



شکل ۵-۱۱ : مقایسه مقادیر بدست آمده برای معیار نسبت توان گذردهی گره های متخاصم از مرجع [۳۹] و مدل ارائه شده در این تحقیق

۵-۳- ارزیابی لایه شبکه

به‌منظور ارزیابی کارایی لایه شبکه بر اساس مدل ارائه شده در بخش ۴-۲ با استفاده از تکنیک ارزیابی مقایسه‌ای از دو معیار ارزیابی **نسبت تحویل بسته**[1] و **تأخیر تحویل انتها به انتها**[2] استفاده شده است. با استخراج مقادیر مرتبط با این دو معیار از مدل SRN ارائه شده و شبیه‌ساز NS-2 کارایی لایه شبکه و پروتکل مسیریابی AODV به ازای اعمال حملات سیاه‌چاله و انهدام بسته ارزیابی شده است. نسبت تحویل بسته (PDR) درصد بسته‌های داده‌ای را بیان می‌کند که در مقابل نرخ بسته ورودی به‌درستی به گره بعدی تحویل داده می‌شوند. بسته‌های ورودی شامل بسته‌های تولیدشده توسط خود گره و بسته‌هایی که توسط دیگر گره‌ها به‌سوی آن فرستاده می‌شود می‌باشد. با این توضیحات، رابطه کلی PDR در معادله ۵-۳ آمده است.

[1] Packet Delivery Ratio(PDR)
[2] End to end Delay

$$PDR = \frac{Thr(T_{send})}{Thr(T_{out})+(Thr(T_{in})\times \Pr(T_{ra}))} \quad (۳-۵)$$

معیار دیگری که مقدار آن را تحت شرایط شبکه در نظر می‌گیریم تأخیر انتها به انتها می‌باشد. این معیار برابر با مدت زمان بین تولید یک بسته داده از سوی گره مبدأ تا زمان دریافت موفقیت آمیز آن توسط گره گیرنده تعریف می‌شود. با داشتن تعداد n گام از مبدأ به سمت مقصد و با استفاده از قانون Little، می‌توان این معیار را به‌صورت معادله ۵-۴ بیان کرد.

$$E\_to\_E\ Delay = \left[\frac{\mathrm{m}(P_{wb})}{Thr(T_{send})}\right] + \left[(n-1)\times\left(\frac{\mathrm{m}(P_{in})}{Thr(T_{send})}\right)\right] \quad (۴-۵)$$

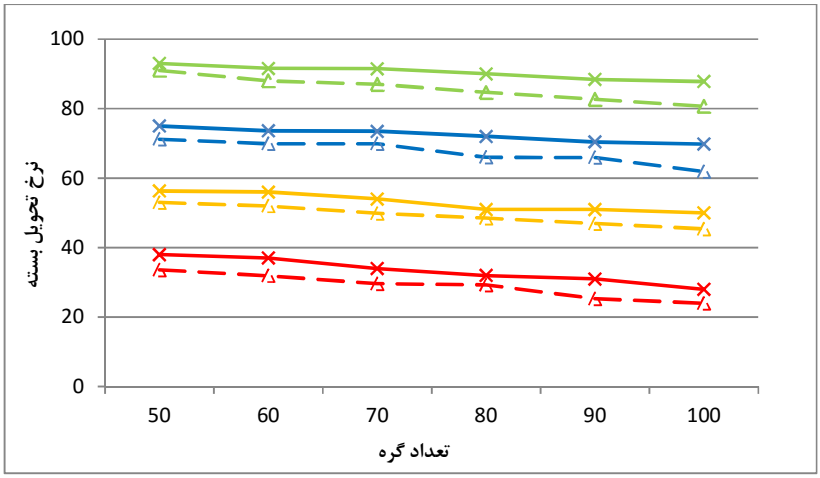
بخش اول از این معادله به زمان موردنیاز برای تحویل یک بسته داده از سوی گره مبدأ به گره بعدی در یک ارتباط یک گامه در طول مسیر به سمت مقصد، اشاره می‌کند. گاهی این زمان، شامل زمان تعمیر و اصلاح مسیر نیز می‌شود که توسط گذار T_{route} انجام می‌شود. زمان ارتباط یک گامه برای n-1 گره بعدی در طول مسیر نیز در بخش دوم این معادله محاسبه شده است.

در ابتدا صحت مقادیر مربوط به تعداد گام جهت رسیدن بسته از مبدأ به مقصد ارائه شده در بخش ۴-۲-۱-۱ با آزمایش‌های متعدد سنجیده شد. سپس برای هر نرخ تولید ترافیک (λ)، مقدار CBR برای مطابقت با این مقدار در شبیه‌ساز NS-2 تنظیم شده است. همچنین مقدار K به‌عنوان پارامتری از مدل SRN، در شکل ۴-۳ به ۶۴ تنظیم شده است که یک مقدار استاندارد می‌باشد. دو معیار عملکرد تحت سه سطح از حملات مورد ارزیابی قرار گرفته‌اند که در آن ۱۰٪، ۱۵٪ و ۲۰٪ از گره‌ها یکی از دو حمله سیاه‌چاله و انهدام بسته را اعمال می‌کنند. در حالت نرمال نیز هیچ گره متخاصمی وجود ندارد. در جمع‌آوری نتایج برای هر معیار کارایی در شبیه‌ساز NS-2، از مقادیر به دست آمده اولیه به علت نوسانات قابل‌توجه مشاهده شده در آن چشم‌پوشی شده است. درمجموع، برای جمع‌آوری هر یک از مقادیر معیارهای کارایی در NS-2 زمان کل مصرفی کاملاً قابل‌توجه بود.

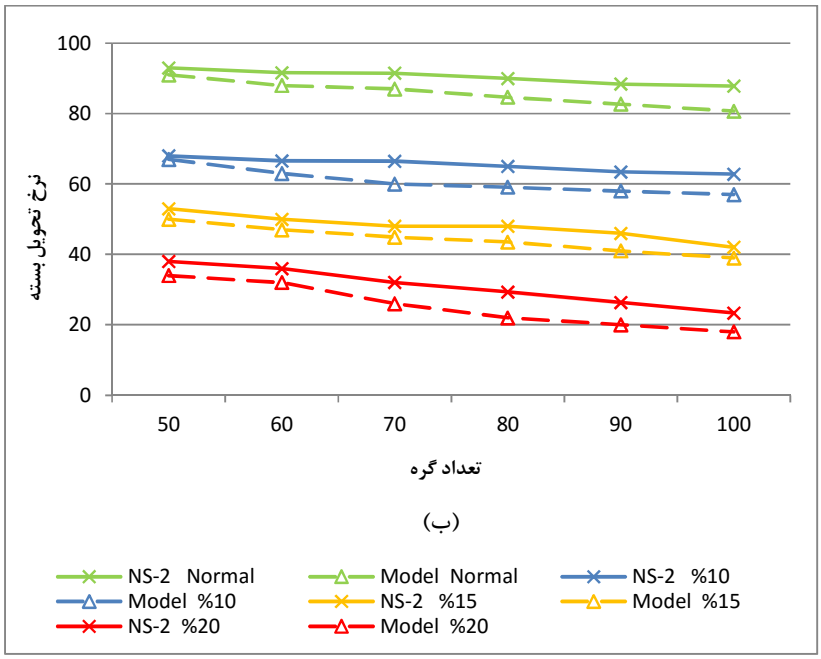
همانند روش استفاده شده برای لایه پیوند داده، دو مدل SRN ارائه شده برای لایه شبکه نیز به‌صورت متداخل تا زمان همگرا شدن یکی از معیارهای ارزیابی به یک مقدار به‌صورت تکراری حل شدند. زمان صرف شده برای به دست آوردن نتایج از مدل SRN ارائه شده نسبت به زمان سپری‌شده برای استخراج معیارها از NS-2 کاملاً قابل‌اغماض بود.

شکل‌های ۵-۱۲ (الف) و (ب) مقادیر به دست آمده برای معیار کارایی (PDR) به ترتیب به ازای دو استراتژی حمله سیاه‌چاله و انهدام بسته نشان می‌دهد. نتایج بدست آمده برای این معیار در مقابل تعداد گره‌ها، هم برای NS-2 و هم برای مدل SRN رسم شده است. از مقادیر بدست آمده بر می‌آید که حمله سیاه‌چاله تخریب بیشتری را برای شبکه نسبت به حمله انهدام بسته‌ها موجب می‌شود. مقدار PDR برای حمله سیاه‌چاله تقریباً ۱۰٪ کمتر از مقدار PDR به دست آمده برای حمله انهدام بسته است. در بدترین حالت به دست آمده در حمله انهدام بسته‌ها، تنها ۲۵٪ از بسته‌ها به مقصد می‌رسد. این مقدار برای حمله سیاه‌چاله کمتر از این مقدار است. این نتیجه می‌تواند به‌این‌علت باشد که یک گره مهاجم از نوع سیاه‌چاله در فرآیند مسیریابی در مقایسه با گره مهاجم از نوع انهدام بسته‌ها که در این مرحله به‌درستی عمل می‌کند بیشتر سبب جذب مسیر به سمت خود می‌شود. این مسئله باعث تخریب بیشتری برای حمله سیاه‌چاله می‌شود.

البته هر دو حمله در فرآیند انتقال داده‌ها رفتاری مشابه دارند. به‌عنوان نتیجه‌گیری دیگری که از آزمایش‌ها حاصل شده، مشاهده می‌شود که با افزایش تعداد گره‌ها مقدار PDR کاهش خواهد یافت. این مورد می‌تواند به علت افزایش احتمال گذار T_{err} به علت ازدحام کانال در اثر ورود گره‌های بیشتر به یک ناحیه همسایگی باشد.



(الف)



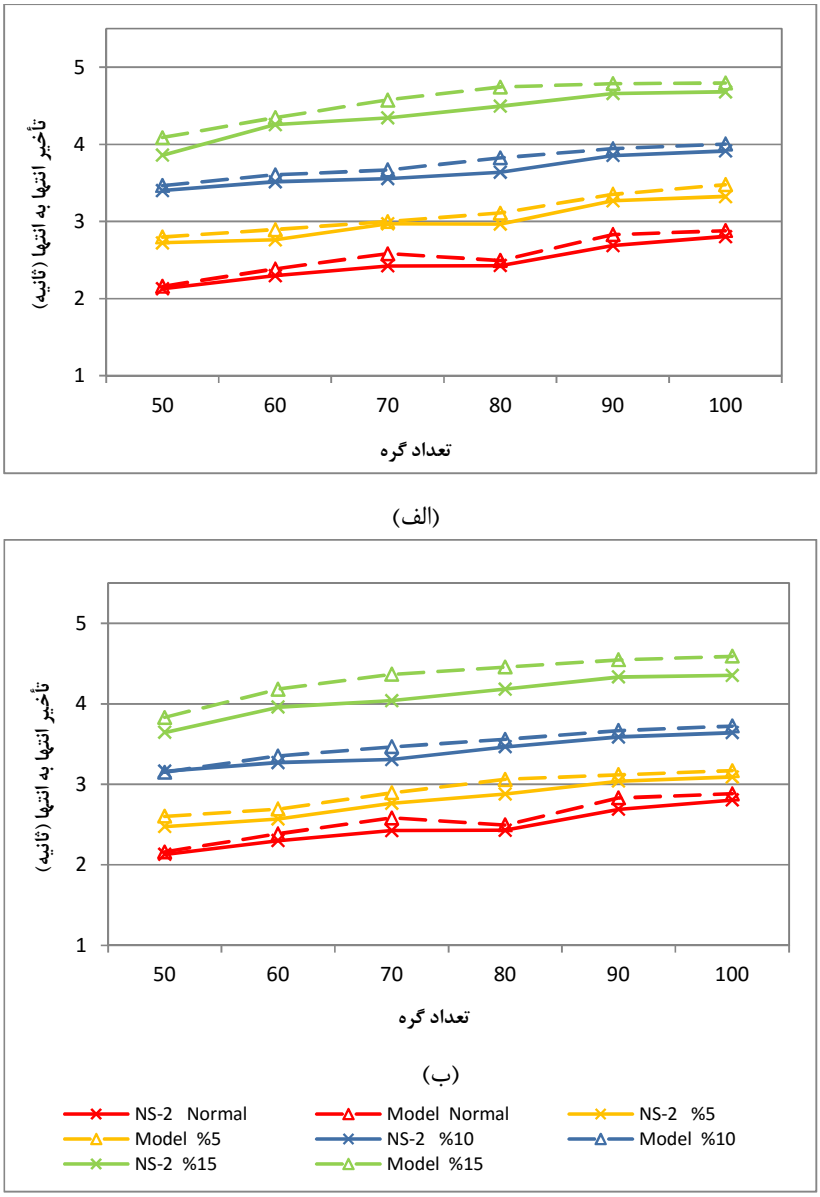
(ب)

شکل ۵-۱۲ ارزیابی نرخ تحویل بسته در لایه شبکه به ازای تعداد گره‌های موجود در اثر اعمال سه سطح از حملات الف) انهدام بسته ب) سیاه‌چاله

معیار تأخیر انتها به انتها به‌عنوان معیاری دیگر، برای ارزیابی دو استراتژی حمله سیاه‌چاله و انهدام بسته‌ها در شکل ۵-۱۳ (الف) و (ب) رسم شده است. همانند نرخ تحویل بسته، برای این معیار نیز افزایش تعداد گره‌ها بطور کلی تأثیر منفی بر روی مقادیرحاصله دارد. با بررسی دقیق‌تر نتایج بدست

آمده مدل SRN مشخص شده است که افزایش تعداد گره‌ها دارای دو پیامد مشخص می‌باشد. در پیامد اول که دارای تأثیر مثبت است، زمان فرآیند مسیریابی که از مدل فرآیند مسیریابی به دست می‌آید کاهش خواهد یافت. این زمان در مدل فرایند جریان داده‌ها به گذار (T_{route}) تخصیص داده شده است. به‌عنوان تأثیری دیگر، افزایش تعداد گره‌ها در یک ناحیه همسایگی احتمال برخورد را تشدید می‌کند. این مسئله تأثیر مستقیمی بر روی احتمال گذار T_{err} دارد و مقدار آن را افزایش می‌دهد.

به نظر می‌رسد که تأثیر منفی مورد آخر در مقایسه با تأثیر مثبت مورد اول غالب باشد که سبب می‌شود با افزایش تعداد گره‌ها، زمان کلی تأخیر انتها به انتها افزایش یابد. برای این معیار نیز حمله سیاه‌چاله نسبت به حمله انهدام بسته‌ها، تأثیر منفی بیشتری را در شبکه ایجاد می‌کند. مشاهده شده است که برای حمله انهدام بسته، در بدترین حالت ۴ تا ۵ ثانیه طول می‌کشد تا یک بسته به مقصد برسد که در آن ۲۰٪ از گره‌ها به‌صورت یک گره متخاصم عمل می‌کنند. این مسئله برای حمله سیاه‌چاله کمی بدتر است. درمجموع، زمان تأخیر انتها به انتها در حمله سیاه‌چاله نسبت به حمله انهدام بسته ۱۰٪ بیشتر طول می‌کشد. در طول ساخت مدل برای حمله سیاه‌چاله: مشاهده می‌شود که مقدار احتمال مربوط به $T_{misbehavior}$ حدود ۱۰ درصد بیشتر از احتمال این گذار در مدل ایجاد شده برای حمله انهدام بسته می‌باشد. همچنین مقدار به دست آمده از مدل SRN و شبیه‌ساز NS-2 روند مشابه‌ای دارند و در اغلب موارد نتایج بدست آمده بر یکدیگر منطبق هستند.



شکل ۵-۱۳ تأخیر انتها به انتها در تحویل بسته در لایه شبکه به ازای تعداد گره‌های موجود در اثر اعمال سه سطح از حملات الف) انهدام بسته ب) سیاه‌چاله

۵-۴- ارزیابی مدل شبکه پتری فازی ارائه شده

به‌منظور پیاده‌سازی روش مسیریابی امن مبتنی بر شبکه پتری فازی ارائه شده بخش ۴-۳ ابتدا اقدام به اضافه نمودن توابع فازی مربوطه به توابع کتابخانه NS-2 نمودیم. با پیاده‌سازی سناریو توضیح داده

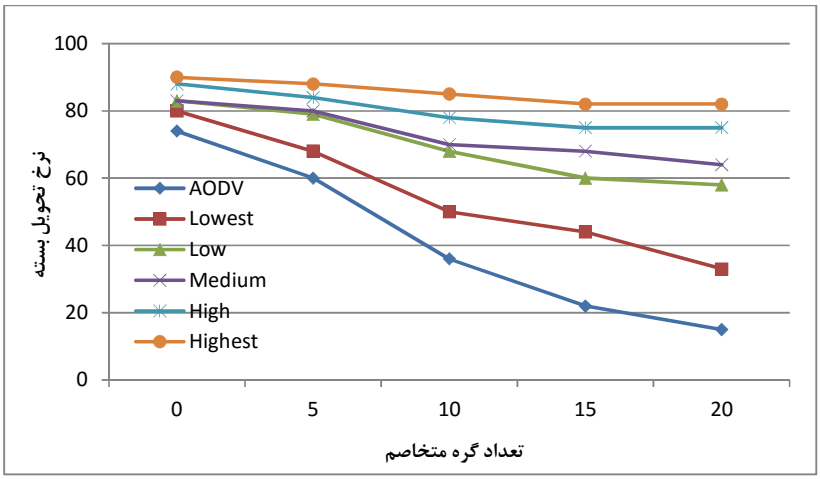
شده در بخش ۵-۱ در هر آزمایش فرض شده که تعداد ۸۰ گره در شبکه وجود داشته باشد. همچنین مدل گره‌های متخاصم به نحوی انتخاب شده که انواع حملات را انجام دهند. مانند حمله سیل‌آسا، حمله سیاه‌چاله، حمله انهدام بسته و به‌روزرسانی جعلی. هر آزمایش در شش حالت انجام شده است بطوریکه در یک حالت از پروتکل پایه AODV استفاده شده و در پنج حالت دیگر، پروتکل اصلاحی با در نظر گرفتن یکی از پنج سطح آستانه امنیتی (کمترین، کم، متوسط، بالا و بالاترین) اجرا و بررسی شده است. برای ارزیابی پروتکل امن مبتنی بر شبکه پتری فازی ارائه شده، معیارهای نسبت تحویل بسته، متوسط SL[1] گره‌ها و درصد گره‌های تشخیص درست[2] / نادرست[3] استفاده خواهند شد. شکل ۵-۱۴ نتایج مربوط به معیار نرخ تحویل بسته را نشان می‌دهد. همان‌طور که در این شکل مشاهده می‌شود، نرخ تحویل بسته در پروتکل اصلاحی ارائه شده نسبت به AODV اصلی بسیار بالاتر است. چیزی که برای این معیار مشهود است رکود چشمگیر در AODV اصلی با افزایش تعداد گره‌های مخرب است. این روند تا حدودی برای مقدار آستانه کمترین نیز صادق است. در سایر موارد با افزایش تعداد گره‌های مخرب یک وضعیت، با روند ثابتی مواجه می‌شویم. بنابراین با استفاده از سطح مناسبی از حداقل مقدار آستانه امنیت، افزایش تعداد گره‌های مخرب، در نسبت تحویل بسته در پروتکل امن مبتنی بر فازی پتری تأثیر چندانی نمی‌گذارد. به نظر می‌رسد که در AODV اصلی، برای ۲۰ گره مخرب تنها ۱۵% درصد از بسته‌ها به مقصد می‌رسند.

متوسط سطح امنیت ((Security Level(SL) معیار دیگری است که در این تحقیق اندازه‌گیری شده است. این معیار در هر دو پروتکل، تنها بر روی گره‌های مشروع محاسبه شده است. در پروتکل امن مبتنی بر شبکه پتری فازی میانگین SL گره‌ها، در بدترین حالت در سطح متوسط است. اما در

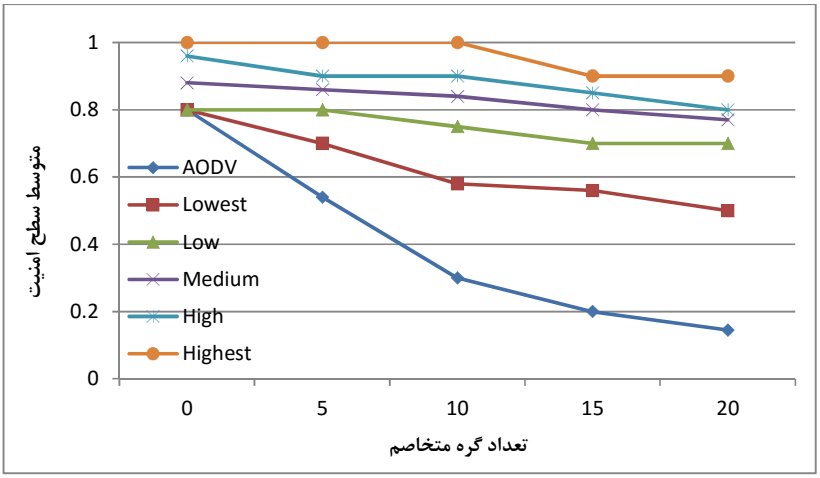
[1] Security Level (SL)
[2] Percentage of True Detector Node (PTDN)
[3] Percentage of False Detector Node (PFDN)

AODV اصلی، با افزایش تعداد گره‌های مخرب کاهش قابل‌توجهی در متوسط SL داریم. این کاهش ادامه می‌یابد تا زمانی که برای ۲۰ گره مخرب با کمترین متوسط SL مواجه خواهیم شد. نتایج در شکل ۵-۱۵ قابل مشاهده و بررسی خواهد بود.

PTDN: این معیار معرف درصد گره‌هایی است که به‌درستی وقوع حمله در شبکه را تشخیص داده‌اند و از تحویل و یا دریافت بسته به یک نود متخاصم امتناع می‌کنند. این امتناع نتیجه مستقیم عملکرد تابع وارسی امنیت گره به گره است که جزئیات آن در بخش ۴-۳-۱ بیان شده است. با توجه به اینکه در عملکرد AODV اصلی، هیچ مکانیزم امنیتی وجود ندارد بنابراین این معیار تنها برای پروتکل امن مبتنی بر شبکه پتری فازی محاسبه شده است. شکل ۵-۱۶ جزئیات نتایج را برای تمام سطوح آستانه امنیت نشان می‌دهد. همان‌طور که در شکل مشخص است برای بالاترین سطح آستانه امنیت، مقدار به دست آمده حدود ۱۰۰ درصد است. نتایج آستانه SL در سطوح بالا و متوسط تا حدودی مشابه سطح بالاترین است. اما در سطوح پایین و یا پایین‌ترین، کاهش قابل‌توجهی در مقدار آستانه شاهدیم.

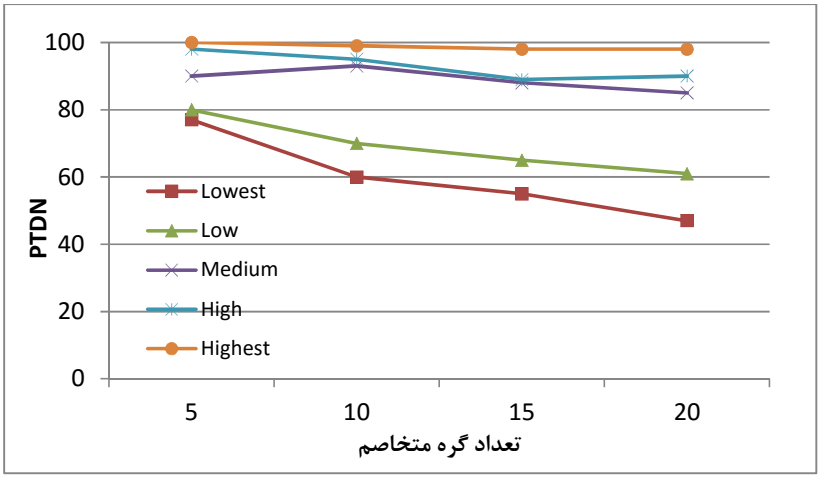


شکل ۵-۱۴ نسبت تحویل بسته برای تمام سطوح آستانه امنیتی در پروتکل امن مبتنی بر شبکه پتری فازی و AODV اصلی در مقابل تعدادی از گره‌های متخاصم.

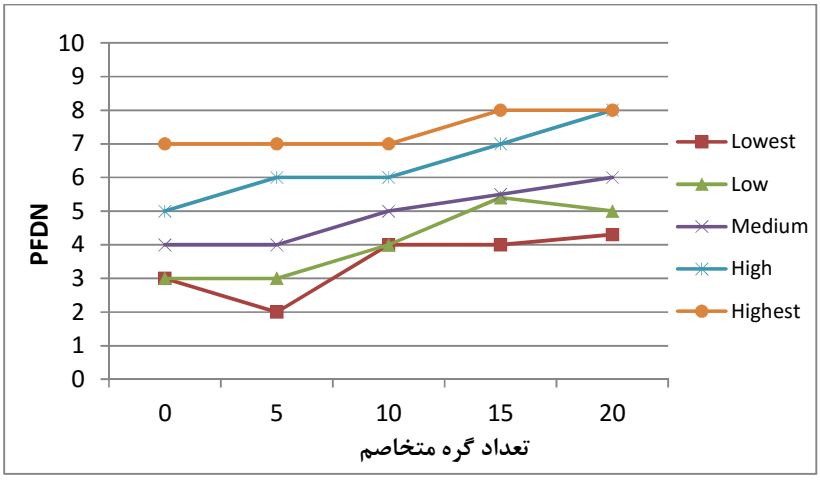


شکل ۵-۱۵: متوسط سطح امنیت برای تمام سطوح آستانه امنیتی در پروتکل امن مبتنی بر شبکه پتری فازی و AODV اصلی در مقابل تعدادی از گره‌های متخاصم.

در شکل ۵-۱۷، نتایج معیار PFDN آمده که نشان‌دهنده درصد گره‌هایی است که تشخیص نادرست را برای یک گره مشروع داده‌اند نشان می‌دهد. این معیار به گره‌هایی اشاره می‌کند که از ارائه بسته به گره‌های مشروع امتناع می‌کنند. همان‌طور که در این شکل مشهود است در این معیار، رسیدن به مقدار بالاتر می‌تواند به دلیل رویکرد محافظه‌کارانه در ارائه بسته باشد (انتخاب آستانه SL در سطح بالا و یا بالاترین). همان‌طور که در شکل مشاهده می‌شود آستانه SL در سطح بالاتر، سبب مقادیر بیشتری از PFDN می‌شود. برای بالاترین سطح آستانه، بالاترین مقدار PFDN و برای پایین‌ترین سطح آستانه، کمترین مقدار PFDN را داریم.



شکل ۵-۱۶: نتایج معیار PTDN برای تمام سطوح آستانه امنیتی در پروتکل امن مبتنی بر شبکه پتری فازی در مقابل تعدادی از گره‌های متخاصم.



شکل ۵-۱۷: نتایج معیار PFDN برای تمام سطوح آستانه امنیتی در پروتکل امن مبتنی بر شبکه پتری فازی در مقابل تعدادی از گره‌های متخاصم.

فصل ۶– نتیجه‌گیری و پیشنهاد کارهای آتی

در این تحقیق به ارائه یک چارچوب تحلیلی برای مطالعه اثرات حملات لایه پیوند داده ولایه شبکه، بر شبکه‌های موردی سیار پرداخته شده است. در ارائه چارچوب مورد نظر از مدل شبکه پتری احتمالاتی مبتنی بر پاداش (SRN) استفاده شده است. انتخاب این ابزار مدل‌سازی به دلیل قابلیت‌های آن در توصیف مواردی مانند فعالیت‌های زمان‌دار، تابع احتمال انتخاب، تعیین شرایط اجرای یک گذار، تعیین وزن‌های چندگانه برای یک کمان و تعیین تابع پاداش برای ارزیابی یک مدل می‌باشد. با توجه به اینکه غالب حملات و ارزیابی‌های صورت گرفته پیشین در شبکه‌های موردی سیار مربوط به لایه‌های شبکه و پیوند داده می‌باشد، در ارائه چارچوب مورد نظر نیز به مدل‌سازی این دو لایه اکتفا شده است. با توجه به پیچیدگی گسترده عملیات موجود در پروتکل‌های شبکه‌های موردی سیار سعی شده تا حد ممکن از ایده تجزیه مدل‌ها [۷۱] و استفاده از رویکرد حل تکراری برای آن استفاده شود. با استفاده از این رویکرد از مشکل انفجار حالت‌ها که مسئله بغرنجی در مدل‌سازی سیستم‌های پیچیده‌ای مانند شبکه‌های موردی سیار است، جلوگیری شده است.

در تعیین صحت مدل ارائه شده از روش ارزیابی مقایسه‌ای استفاده شده است. در این روش با تشریح یک سناریو با پارامترهای آن اقدام به پیاده‌سازی آن در شبیه‌ساز NS-2 و تفسیر مقادیر در مدل SRN شده است. سپس، با استخراج یکسری از معیارهای ارزیابی به بررسی نتایج اقدام شده است. با توجه به اینکه در روش تحقیق و پیاده‌سازی آن اقدام به ارائه مدل جداگانه برای هریک از لایه‌های پیوند داده و شبکه نمودیم در این بخش نیز به بررسی هرکدام به‌صورت جداگانه خواهیم پرداخت. همچنین مدل شبکه فازی پتری ارائه شده برای یک مسیریابی امن نیز در ادامه بررسی خواهد شد.

۶-۱- بررسی لایه پیوند داده

همان‌طور که در بخش ۴-۱ توضیح داده شد ارائه مدل در لایه پیوند داده مبتنی بر دو مدل مجزا با نام‌های مدل جزئی گره‌ها و مدل برهم‌کنش گره‌ها صورت گرفت است. اولی ناظر بر فعالیت‌های صورت گرفته در یک گره جهت انتقال داده در یک کانال مشترک مطابق با پروتکل IEEE 802.11 DCF

می‌باشد. مدل برهم‌کنش گره‌ها نیز نحوه تعامل و تأثیر متقابل گره‌های موجود در یک فضای همسایگی را مدل نموده است. مدل برهم‌کنش گره‌ها به نحوی طراحی شده است که عملکرد گره‌های متخاصم را علاوه بر گره‌های مشروع نشان دهد. در این مدل پارامترهای مرتبط با گره‌های متخاصم به نحوی متفاوت با گره‌های مشروع می‌باشد. همچنین با توجه به تأثیر مهم گره‌های موجود در ناحیه مخفی در عملکرد گره‌های موجود در یک همسایگی، تأثیر متقابل این گره‌ها نیز در ارسال داده‌ها محاسبه شده است.

کارهای پیشین که اقدام به مطالعه شبکه‌های موردی سیار با استفاده از مدل‌سازی تحلیل نمودند غالباً فرض را بر وجود یک شبکه ثابت با تعدادی گره مشخص قرار دادند. اما مدل ارائه شده برای لایه پیوند داده در این تحقیق، قابلیت کار با هر مقیاس از شبکه و هر تعداد گره را به‌صورت پویا دارد. این کار از طریق محاسبه روابط ریاضی جهت مشخص نمودن تعداد گره‌های موجود در یک ناحیه همسایگی و تعداد گره‌های موجود در ناحیه مخفی را دارد. در محاسبات انجام شده فرض شده است که گره‌ها از مدل حرکتی RWP تبعیت می‌کنند.

برای ارزیابی مدل ارائه شده از روش ارزیابی مقایسه‌ای استفاده شده است. بر اساس این روش، سناریوهایی با تعداد گره‌های متفاوت از ۴۰ تا ۱۰۰ و همچنین سه نرخ تولید داده متفاوت شامل ۳۰۰ کیلوبایت بر ثانیه، ۶۰۰ کیلوبایت بر ثانیه و یک مگابایت بر ثانیه با اعمال چهار حمله متفاوت در لایه پیوند داده در شبیه‌ساز NS-2 پیاده‌سازی شده است. همچنین مشخصات سناریوها در مدل‌های ارائه شده برای لایه پیوند داده تفسیر شده‌اند. نتایج با استخراج دو معیار ارزیابی **تأخیر ارسال یک گامه** و **توان گذردهی لایه پیوند داده** ارزیابی شده‌اند که حاکی از برابری نتایج دو محیط و صحت مدل ارائه شده بوده است.

در حل مدل تحلیلی ارائه شده، از روش حل تکراری تا زمان همگرایی آن به یک مقدار خاص استفاده شده است. همچنین با توجه به نوسان مشاهده‌شده در نتایج به‌دست‌آمده از شبیه‌ساز NS-2 مجبور به پیاده‌سازی و استخراج مقادیر ارزیابی به اندازه پنج مرتبه شده‌ایم که برای این کار زمان زیادی صرف شده است. در مقابل، نتایج مربوط به مدل در مدت زمان بسیار کوتاهی استخراج شده است. همچنین بعد از اطمینان از صحت مدل ارائه شده اقدام به ارزیابی شبکه بر اساس میزان درصد تصرف کانال توسط گره‌های مشروع و متخاصم و همچنین میزان آزاد بودن کانال شده است.

از نتایج بدست آمده از چهار حمله در نظر گرفته شده در لایه پیوند داده شامل حمله دست‌کاری بازه انتظار تعویق (CW)، حمله کاهش بازه انتظار DIFS، حمله دست‌کاری بردار NAV و حمله دست‌کاری سرعت انتقال، اینطور برمی‌آید که دو حمله اولیه دارای قدرت تأثیرگذاری بیشتری هستند. همچنین نشان داده شده است که حمله دست‌کاری بازه انتظار تعویق (CW) در شرایط ازدحام که تعداد گره‌های بیشتری در شبکه وجود دارد و نرخ انتقال داده نیز بیشتر است قدرت تخریب بیشتری پیدا می‌کند. به‌طورکلی به نظر می‌رسد سیاست خودخواهانه در مقابل سیاست خصمانه در پروتکل IEEE 802.11 DCF دارای قدرت کارکرد بیشتری است و این نشان‌دهنده مکانیزم صحیح این پروتکل در لایه پیوند داده است.

۶-۲- بررسی لایه شبکه

بر اساس ایده تجزیه مدل‌ها، فعالیت‌های موجود در لایه شبکه نیز بر اساس دو مدل مجزا ارائه شده است. یک مدل برای جریان انتقال داده و یک مدل نیز برای نشان دادن فرآیند مسیریابی که با فرض استفاده از الگوریتم مسیریابی AODV طراحی شده است. مدل جریان داده نمایش‌دهنده فعالیت‌های صورت گرفته در یک گره به‌منظور انتقال داده است. داده انتقال داده شده توسط یک گره می‌تواند توسط خود آن گره تولیدشده و یا آن‌که داده دریافتی از گره‌های دیگر باشد که به‌جهت انتقال به گره بعدی در مسیر با استفاده از پروتکل مسیریابی ایجاد شده است. مدل فرآیند مسیریابی نیز نشان‌دهنده

مجموعه فعالیت‌های صورت گرفته در پروتکل مسیریابی AODV مانند ارسال و دریافت RREQ، ارسال و دریافت RREP و ادامه فرآیند مسیریابی به اندازه TTL بار می‌باشد.

در تعیین پارامترهای مرتبط با مدل در این لایه نیازمند تعیین مشخصه‌هایی بوده‌ایم. از جمله این مشخصه‌ها، فرکانس خرابی و بازیابی مسیر، احتمال غیر معتبر بودن مسیر موجود در جدول مسیریابی یک گره، نرخ داده دریافتی از گره‌های دیگر جهت انتقال به مقصد، تعداد گام موردنیاز جهت دستیابی به مقصد و همچنین تعداد گام طی شده جهت رسیدن به گرهی است که در جدول مسیریابی خود اطلاعی از مقصد دارد، می‌باشد. بعضی از مشخصه‌های مذکور با استفاده از روابطی از دل مدل استخراج شده و برای بعضی دیگر لازم به محاسبه روابط ریاضی مرتبط بوده است. به‌عنوان‌مثال، محاسبه تعداد گام جهت رسیدن از مبدأ به مقصد با استفاده از روابط ریاضی ارائه شده در بخش ۴-۲-۱-۱ و محاسبه فرکانس و احتمال خرابی مسیر با استفاده از نتایج تحقیق انجام‌شده در [۵۹ و ۶۱] به‌دست‌آمده است. همچنین برخی از پارامترهای موجود در مدل لایه شبکه مانند مدت زمان لازم جهت انتقال یک گامه در کانال نیز از مدل ارائه شده جهت لایه پیوند داده استخراج شده است.

در فاز ارزیابی نیز مشابه با مدل پیوند داده از روش ارزیابی مقایسه‌ای استفاده شده است. در سناریو پیاده‌سازی شده عملکرد لایه شبکه با پیاده‌سازی سه سطح از اعمال حملات **سیاه‌چاله** و **انهدام بسته‌ها** در شبیه‌ساز NS-2 و مدل ارائه شده، ارزیابی شده است. به‌منظور ارزیابی از معیارهای **تأخیر انتها به انتها** و **نرخ تحویل بسته** استفاده شده است. مقادیر به‌دست‌آمده نشان‌دهنده برابری نتایج دو محیط بوده و همچنین نشان داده شده است که حمله سیاهچاله دارای قدرت تخریب بیشتری نسبت به حمله انهدام بسته‌ها می‌باشد. زمان تحلیل و استخراج نتایج این مدل نیز در مقایسه با شبیه‌ساز NS-2 بسیار ناچیز بوده است

۶-۳- بررسی مسیریابی امن مبتنی بر شبکه پتری فازی

همان‌طور که در بخش ۴-۳ توضیح داده شد در تلاش دیگر سعی شد تا پیوندی را بین مدل‌سازی تحلیلی و محیط شبیه‌سازی ایجاد کنیم. به همین منظور با توجه به ماهیت فازی اکثر فعالیت‌های صورت گرفته در شبکه‌های موردی سیار از ابزار مدل‌سازی تحلیلی شبکه پتری فازی استفاده شده است. همانند آنچه در مدل مبتنی بر شبکه پتری فازی برای فعال شدن یک گذار وجود دارد، از چهار متغیر فازی برای فعال شدن یک اتصال ارتباطی جهت انتقال داده استفاده می‌شود. الگوریتم مسیریابی امن ارائه شده مبتنی بر دو فاز وارسی امنیت گره به گره و وارسی امنیت کل مسیر بوده است که اولی در صورت کمتر بودن مقدار متغیر فازی خروجی مرتبط با سطح امنیت اتصال ارتباطی بین دو گره از یک حد خاص مانع از انتقال داده بین دو گره خواهد شد. فاز وارسی امنیت کل مسیر نیز به دنبال پیدا کردن مسیر با سطح امنیت بالاتر از میان مسیرهای موجود به سمت مقصد می‌باشد.

با پیاده‌سازی توابع فازی مورد نظر در شبیه‌ساز NS-2 مجبور به اعمال تغییراتی در ساختار جدول مسیریابی گره‌ها، سرآیند بسته RREQ و سرآیند بسته RREP در پروتکل مسیریابی AODV شده‌ایم. همچنین یک جدول مسیریابی دیگر جهت پایش متغیرهای فازی همسایگان به پروتکل AODV افزوده شد. عملکرد پروتکل ارائه شده با تعیین پنج سطح آستانه امنیت لینک ارتباطی بین گره‌ها در مقایسه با پروتکل AODV مقایسه شد. به‌منظور مقایسه نیز از معیارهای نرخ تحویل بسته و متوسط سطح امنیت گره‌ها، تعداد گره‌های تشخیص‌دهنده درست و تعداد گره‌های تشخیص‌دهنده نادرست استفاده شد. در سناریو شبیه‌سازی‌شده تعداد ۸۰ گره وجود داشت که ۱۵٪ آن‌ها شامل گره‌های متخاصم بوده‌اند که اقدام به انجام فعالیت‌های مثل انهدام بسته‌های داده و یا تولید بسته‌های REEQ بیش اندازه و جعلی، به‌روزرسانی غیرمعتبر جدول مسیریابی و سیاست حمله سیاهچاله می‌کنند

۶-۴- محدودیت‌های تحقیق و راهبرد آینده

قطعاً تحقیق ارائه شده دارای محدودیت‌هایی می‌باشد که می‌تواند در آینده توسط محققان دیگر به‌عنوان ادامه کار مورد بررسی قرار بگیرد. در ذیل به این موارد پرداخته خواهد شد.

- در محاسبات ریاضی ارائه شده برای مدل‌های SRN لایه پیوند داده و شبکه (بخش‌های ۴-۲ و ۴-۳)، مانند تعداد گره‌های موجود در یک همسایگی و یا تعداد گام‌های لازم برای ارسال داده از مبدأ تا مقصد فرض بر استفاده از مدل حرکتی RWP برای گره‌ها قرار گرفته است. در صورت پیروی گره‌های موجود در شبکه از مدل‌های حرکتی دیگر مانند Random Walk، Manhatan، Uniform و امثال آن لازم است محاسبات دیگری انجام شود.
- مطابق با گفته‌های بالا در محاسبات مذکور فرض شده است که گره‌ها در یک فضای مربع گونه درحرکت هستند که در صورت متفاوت بودن با این مورد لازم است تا محاسبات دیگری صورت گیرد.
- به نظر می‌رسد که مدل ارائه شده جهت لایه شبکه از توانایی لازم جهت رصد فعالیت یکسری از حملات این لایه را نداشته باشد. البته دلیل این مورد را می‌توان به سطح انتزاع بالای فعالیت‌های موجود در این لایه نسبت داد که سبب می‌شوند فعالیت‌های این لایه دارای پیچیدگی احتمالاتی بالایی باشند. به اعتقاد نگارنده در این خصوص لازم به ارائه مدل دقیق‌تر(با سطح انتزاع پایین تر) با ذکر جزئیات بیشتری خواهد بود که برای جلوگیری از مشکل انفجار حالت‌ها در تحلیل آن شاید نیاز به استفاده از مدل‌های دیگر شبکه پتری مانند پتری رنگی باشد.
- همچنین آن‌طور که از نتایج بر می‌آید، مقادیر بدست آمده برای مدل SRN لایه شبکه در بعضی موارد از انطباق کمتری با نتایج مستخرج از شبیه ساز NS-2 نسبت برخوردار بوده است. در توجیه این مورد می‌توان به موارد ذکر شده در بالا و همچنین استفاده از پارامترهایی

در مدل اشاره کرد که از نتایج تحقیقات دیگر بوده است. از جمله می‌توان به محاسبه نرخ و احتمال خرابی مسیر و همچنین اندازه جدول مسیریابی اشاره کرد.

- تأثیر متداخل و هم‌زمان حملات لایه پیوند داده و شبکه در تحقیق ارائه شده مورد ارزیابی قرار نگرفته است.
- مدل SRN پیشنهادی در این تحقیق تنها با هدف ارزیابی کارایی شبکه‌های موردی سیار در دو لایه پیوند داده و شبکه در شبکه‌های موردی سیار ارائه شده است. بعنوان یک راهبرد آینده پیشنهاد می‌شود با افزودن الگوریتم‌های هوشمند که قابلیت مدل‌سازی و اضافه شدن به یک مدل پتری دارند در ارتباط با نحوه ارتقاء سطح امنیتی و جلوگیری از اعمال حملات در هر لایه تحقیق شود. برای این منظور می‌توان از الگوریتم‌هایی مانند تئوری بازی‌ها، شبکه عصبی و امثال آن به‌عنوان یک لایه کنترل نظارتی[1] در سطح بالاتری از مدل هر لایه استفاده کرد. همچنین در این ارتباط می توان از راهبردهای غیرهوشمند بصورت تکنیکی جهت جلوگیری از اعمال حملات نیز استفاده کرد.

[1] Supervisory control

فهرست منابع

[1] Ben Saieda Y., Olivereaua A., Zeghlacheb D., Laurent M. (2014) “A survey of collaborative services and security-related issues in modern wireless Ad-Hoc communications”, J network comput appl, 45 , PP 215–227.

[2] Maity S., Hansdah R.C, (2014) “Self-organized public key management in MANETs with enhanced security and without certificate-chains”, J. Computer Networks, 65, PP 183–211

[3] Moamen A. A., Hamza, H. S. and Saroit, I. A., (2013) “Secure multicast routing protocols in mobile ad-hoc networks”. Int. J. Commun. Syst., 27, 11, PP 2808–2831.

[4] Mitchell R., Chen I. (2014) "A survey of intrusion detection in wireless network applications", Comput Commun , 42, PP 1–23

[5] Mokdad L., Ben-Othman J., Yahya B., Niagne S. (2016) ” Performance evaluation tools for QoS MAC protocol for wireless sensor networks”, Ad Hoc Netw, 12, PP 86-99.

[6] Cavin D., Sasson Y., Schiper A.,(2002) “On the Accuracy of MANET Simulators”. in: Proceedings of ACM POMC02,P38, Toulouse, France,.

[7] Macia1 H, Ruiz. M. C., Mateo J. A., Calleja J. L., (2015) ” Petri nets-based model for the analysis of NORIA protocol”, Concurrency Computat.: Pract. Exper, 27(17), PP 4704–4715.

[8] Schoch E., Feiri M., Kargl F., Weber M. (2008) “Simulation of adhoc networks: ns-2 compared to JiST/SWANS”, International Conference on Simulation Tools and Techniques for Communications, Networks and Systems, P36, Marseilles, France.

[9] M. Takai, J. Martin, R. Bagrodia, (2001) “Effects of Wireless Physical Layer Modeling in Mobile Ad Hoc Networks,” In Proceedings of MobiHooc, P87, Long Beach, CA.

[10] Silvaa E and P. Albinib L. (2014),"Middleware proposals for mobile ad hoc networks", J network comput appl, 43, PP 103–120

[11] Andel, Todd R., (2007) "Formal Security Evaluation of AD HOC Routing Protocols". ProQuest. Paper.

[12] Sheikh R., Singh Chande M., Kumar Mishra D., (2010) “Security issues in MANET: A review” International Conference On Wireless And Optical Communications Networks (WOCN), P1,Colombo, Sri Lanka

[13] Barbeau M., Kranakis E. (2007), “Principles of ad hoc networking”, John Wiley and Sons.

[14] Stallings W., (2005), “Wireless Communications and Networks”, Prentice Hall,.

[15] Murthy C. S. R., Manoj B. S, (2004) ” Ad Hoc Wireless Networks: Architectures and Protocols: Prentice Hall.

[16] Mokdad L., Ben-Othman b J., Yahya B., Niagne S., (2016) ” Performance evaluation tools for QoS MAC protocol for wireless sensor networks”, Ad Hoc Networks 12 , PP 86-99.

[17] Yadollahzadeh Tabari M, Hassanpour H, Pouyan A, Saleki S. (2012) “Proposing a light weight semi-distributed IDS for mobile ad-hoc network based on nodes’ mode”. 6Th International Symposium on Telecommunication (IEEE), P948, Tehran, Iran.

[18] Wang B., Song F., Zhang S., Zhang H., (2008), “Throughput modeling analysis of IEEE 802.11 DCF mechanism in multi-hop non-saturated wireless ad-hoc networks”, International Conference on Communications, Circuits and Systems, P383, Fujian, Chinese.

[19] Fangqin L., Chuang L., Hao W., Peter U., (2009) “Throughput Analysis of Wireless Multi-hop Chain Networks,” IEEE/ACIS International Conference on Computer and Information Science, P834, Shanghai, Chinese.

[20] Ahmad Ali A., Fayez G., Lin C., (2009) “Modeling the throughput and delay in wireless multihop ad hoc networks,” in the IEEE conference on Global telecommunications, Honolulu, P1, Hawaii, USA.

[21] Charles E. P., Pravin B.,(1994) “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers,” ACM Conference on Communications Architectures, Protocols and Applications, P 234, New York, NY, USA.

[22] Chiang C.-C., (1997) "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel". IEEE SICON'97, P197,

[23] Johnson D., Maltz D., Hu Y. C., (2007) “The Dynamic Source Routing for mobile ad hoc networks” RFC 4728, The Internet Engineering Task Force, Network Working Group, http://www.ietf.org/rfc/rfc4728.txt.

[24] Perkins C., Belding-Royer E., Das S. (2003), “Ad hoc On-Demand Distance Vector (AODV) Routing”, RFC 3561, The Internet Engineering Task Force, Network Working Group , https://www.ietf.org/rfc/rfc3561.txt.

[25] F.-C. Jiang et al, (2014) ”A Petri Net Design toward Prolonging Operational Lifetime of Ad Hoc Networks under Flooding Attack”, Ubiquitous Information Technologies and Applications, Lecture Notes in Electrical Engineering, Springer Berlin Heidelber, PP 123-130.

[26] Jianga F, Lina C, Wub H, (2014) "Lifetime elongation of ad hoc networks under packet dropping attack using power-saving technique", Ad Hoc Netw, 21, PP 84–96

[27] Baadache a, Belmehdi A, (2014) “Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks", Computer Networks, 73, PP 173-184.

[28] Ming-Yang Su, (2010) “WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks”, Computers & Security 29(2), PP 208–224.

[29] Xu K., Gerla M., Bae S., (2003) “Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks,” Ad Hoc Networks, 1(1), PP 107-123,

[30] Younes O., Thomas N. (2011) “An SRN Model of the IEEE 802.11 DCF MAC Protocol in Multi-Hop Ad Hoc Networks with Hidden Nodes”. The Computer Journal, 54,PP 875- 893

[31] Sanandaji, A., Jabbehdari, S., Balador, A., & Kanellopoulos, D. (2013). MAC layer misbehavior in MANETs. IETE Technical Review, 30(4), PP 324–335.

[32] Kartson D., Balbo G., Donatelli S., Franceschinis G., Giuseppe C, (1994) “Modelling with Generalized Stochastic Petri Nets”, John Wiley and Sons

[33] German R., Heindl A., (1999), “Performance evaluation of IEEE 802.11 wireless LANs with stochastic Petri nets,” International Workshop on Petri Nets and Performance Models, PP 44, Zaragoza, Spain

[34] Xudong H., Murata T., (2005) ”High-Level Petri Nets—Extensions, Analysis, and Applications”, Electrical Engineering Handbook (ed. Wai-Kai Chen), Elsevier Academic Press, PP 459-476.

[35] Trivedi K.S , Tomek L.A, (1995) “Analyses Using Stochastic Reward Nets” Software fault tolerance , Wiely Publication, PP 139-166.

[36] Pouyan A. A. and Tabari M. Y, (2015).” FPN-SAODV: using fuzzy petri nets for securing AODV routing protocol in mobile Ad hoc network, Int. J. Commun. Syst.,

[37] Bianchi G. (2000) “Performance analysis of the IEEE 802.11 distributed coordination function,” IEEE Journal on Selected Areas in Communications, 18(3), pp. 535-547,

[38] Jianhua H., Dritan K., Alistair M., Yiming W., Angel D., Joe M., Zhong F.,(2005) “Performance investigation of IEEE 802.11 MAC in multihop wireless networks,” in ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, P242 Montrial, Quebec, Canada,.

[39] Lei Guang, Assi C., Benslimane A. (2006)” Modeling and analysis of predictable random backoff in selfish environments”, 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems, P 86, New York, NY, USA

[40] Lei Guang, Assi C., Benslimane A. (2006).,” Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks”, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, P 116, Montreal, Canada

[41] Lei Guang, Assi C., Benslimane A. (2008) ,” Enhancing IEEE 802.11 Random Backoff in Selfish Environments”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 57(3), PP 1806-1822.

[42] Raya, M., Aad, I., Hubaux, J.P. and El Fawal, A., (2006) “DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots”. IEEE Transactions on Mobile Computing, 5(12), PP 1691-1705.

[43] P. Kyasanur, (2005) ”Selfish MAC Layer Misbehavior in Wireless Networks”, IEEE TRANSACTIONS ON MOBILE COMPUTING,4(5), PP 502-516.

[44] Weng, C.E. and Chen, H.C., (2016). “The performance evaluation of IEEE 802.11 DCF using Markov chain model for wireless LANs”. Computer Standards & Interfaces, 44, pp.144-14

[45] Hadzi-Velkov, Z. and Spasenovski, B.,(2003), “Saturation throughput-delay analysis of IEEE 802.11 DCF in fading channel”, ICC'03. IEEE International Conference on, P 121, Anchorage, AK

[46] Jayaparvathy, R., Anand, S., Dharmaraja, S. and Srikanth, S., (2007). “Performance analysis of IEEE 802.11 DCF with stochastic reward nets”. *International Journal of Communication Systems*, *20*(3), pp.273-296..

[47] Osama Y., Nigel T., (2011) " An SRN Model of the IEEE 802.11 DCF MAC Protocol in Multi-Hop Ad Hoc Networks with Hidden Nodes". The Computer Journal, , (54), 875- 893

[48] Masri, A., Bourdeaud'Huy, T. and Toguyeni, A., (2009). "Performance analysis of IEEE 802.11 b wireless networks with object oriented petri nets.", Electronic Notes in Theoretical Computer Science, 242(2), pp.73-85

[49] Mokdad, L., Ben-Othman, J., Yahya, B. and Niagne, S.,(2014). Performance evaluation tools for QoS MAC protocol for wireless sensor networks. Ad Hoc Networks, 12, pp.86-99..

[50] Zhang, C. and Zhou, M., (2003) "A stochastic Petri net-approach to modeling and analysis of ad hoc network", ITRE2003. International Conference on Research and Education, P152, NJ, USA

[51] Huang, H. and Zhou, Q., 2012, July. Petri-net-based modeling and resolving of black hole attack in wmn. In Computer Software and Applications Conference Workshops (COMPSACW), P409, Izmir, Turkish

[52] Alessandro B., (2013) "A Coloured Nested Petri Nets Model for Discussing MANET Properties" International Journal of Multimedia Technology,3(2), PP. 38-44

[53] Xiong, C., Murata, T. and Tsai, J., (2002), "Modeling and simulation of routing protocol for mobile ad hoc networks using colored petri nets.", formal methods in software engineering and defence systems,(12), (PP 145-153).

[54] Meenakshi D., Aakanksha C. (2015)" Modelling and Analysing of Performance of an AODV Routing Protocol Using CPN", International Journal of Advanced Research in Computer Science and Software Engineering, 5(6),

[55] Wang, H.X., Hu, X., Fang, J.C. and Jia, W.J., (2007). "Analysis of reactive routing protocols for mobile ad hoc networks in Markov models". Applied Mathematics and Mechanics, 28, pp.127-139.

[56] Dimitar T., Sonja F., Marija E., Aksenti G., "Ad hoc networks connection availability modeling," in Proceedings of the ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, , 2004, P56. Venezia, Italy

[57] Song, Q., Ning, Z., Wang, S. and Jamalipour, A., (2012). Link stability estimation based on link connectivity changes in mobile ad-hoc networks.Journal of Network and Computer Applications, 35(6), pp.2051-2058.

[58] Chen, D., Garg, S. and Trivedi, K.S., 2002, "Network survivability performance evaluation: a quantitative approach with applications in wireless ad-hoc networks," in the ACM International Workshop on Modeling analysis and simulation of wireless and mobile systems, P61, Atlanta, Georgia, USA,.

[59] Osama Y. and Nigel T. (2012), "A Path Connection Availability Model for MANETs with Ra\'ndom Waypoint Mobility," *European Performance Engineering Workshop* (*EPEW*), P 111, Munich, Germany, July.

[60] Kostin A., Oz G., Haci H., (2014) "Performance study of a wireless mobile ad hoc network with orientation-dependent internode communication scheme". Int. J. Commun. Syst. , 27, PP 322–340.

[61] Osama Y. and Nigel T. (2011), “Analysis of the Expected Number of Hops in Mobile Ad Hoc Networks with Random Waypoint Mobility,” *Electronic Notes in Theoretical Computer Science*, 275, pp. 143-158.

[62] Bettstetter C.,” Stochastic properties of the random waypoint mobility model”, Wireless Networks, 10(5), PP 555 – 567

[63] Bettstetter C. (2004), “On the Connectivity of Ad Hoc Networks,” Computer Journal, 47(4), PP 432-447.

[64] Swades De, (2005) ”On Hop Count and Euclidean Distance in Greedy Forwarding in Wireless Ad Hoc Networks”, IEEE COMMUNICATIONS LETTERS, 9(11), PP 1000-1002

[65] Little, J. D. C. (2011). "Little's Law as Viewed on Its 50th Anniversary" Operations Research, 59 (3), PP 536–549

[66] Bettstetter C , (2003)., “The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks”. IEEE TRANSACTIONS ON MOBILE COMPUTING, 2(3), pp.257-269

[67] J Xu, J., Kumar, A., Yu, X..(2009). “On the Fundamental Tradeoffs Between Routing Table Size and Network Diameter in Peer-to-Peer Networks” IEEE Journal on Selected Areas in Communications. 22,(1), PP 151-163

[68] Ciardo G., Muppala J., Trivedi K., (1989) “SPNP: Stochastic Petri Net Package,” in Proceedings of the Third International Workshop on Petri Nets and Performance Models, pp. 142. Kyoto, Japan.

[69] Mainkar V., Trivedi K. S, (1995) “Fixed point iteration using stochastic reward nets”, Proceedings of the Sixth International Workshop on Petri Nets and Performance Models, P 21, Durham, NC

[70] Ciardo G., Trivedi K. S, (1991) “A decomposition approach for stochastic Petri net models,”in Proceedings of the International Workshop on Petri Nets and Performance Models P74, Melbourne, Vic

[71] M. Ajmone Marsan, G. Balbo, A. Bobbio, G. Chiola, G. Conte, and A. Cumani(1989) "The effect of execution policies on the semantics and analysis of stochastic Petri nets" IEEE Transactions on Software Engineering, 15(7), PP 832–846

[72] Looney, C.G., (1988). "Fuzzy Petri nets for rule-based decisionmaking". *IEEE Transactions on Systems, Man, and Cybernetics*, *18*(1), pp.178-183.

Abstract

Formal and model based analytical methods like petri nets have sufficient facilities for modeling and performance analysis of mobile ad hoc networks. Using these methods for performance analysis of such a system has advantages like speed in parameter extractions, the ability of steady state analysis of a system and providing a visual illustration of its behavior. Also the usage of these methods in designing routing protocols, leads a considerable decline in development time, finding issues and providing a comprehensive evaluation. So in this research we attempt to use analytical modeling tool for performance analysis of mobile ad-hoc network versus operation of misbehavior nodes. We emphasis on two important layers in MANET protocol stack as data-link and network layer.

For the data link layer model, the performance evaluation is done on IEEE 802.11 distributed coordination function (DCF) as a popular media access control (MAC) layer protocol. The goal of this evaluation is to examine this protocol under the existing of misbehavior nodes which selfishly try to grape common channel in a neighbor area. The presented model consists of two separate stochastic reward net (SRN) models. The first model which are called *one node operation model* supposed for presenting all DCF operations in a single node such as Collision Avoidance (CA), RTS/CTS handshake and backoff mechanism. As a next SRN model, *all node operation model*, is used for modeling nodes competition for occupying channel in a neighbor area. The models could be adjusted to a dynamic network with any number of nodes, dimension scale and nodes speed. For evaluation purpose, four distinct attack types implemented by modifying associated transitions in SRN models. The proposed SRN model has been quantified by deriving two performances metrics as *Throughput* and *Delay*. Both metrics are also compared to the value obtained from NS-2 in terms of different number of nodes and three packet generation rates.

The presented framework for the network layer encompasses two separate models: one for analysis of data flow and the other for modeling routing process which is based on AODV routing protocol. To verify the presented model, an equivalence-based method is applied. The proposed SRN model has been quantified by deriving two performances metrics as Packet Delivery Ratio (PDR) and End-to-end Delay. Both metrics are also compared to the value obtained from NS-2 versus different number of nodes and four packet generation rates.

Keyword: mobile ad hoc network, modeling, Petri net, security, attacks

Shahrood university of technology
Faculty of computer and IT Engeeniring

Phd Thesis in aritificial intelligence

Modeling and performance analysis of mobile ad hoc network versus attacks using petri nets

By: Meisam Yadollahzadeh Tabari

Supervisor:
Ali.A Pouyan

Advisor:
A.R Marouzi

August 2016