



ارائه شده توسط:

سایت ترجمه فا

مرجع جدیدترین مقالات ترجمه شده

از نشریات معتبر

## روش مسیر یابی مرکب برای شبکه های ویژه بی سیم

چکیده

برای ایجاد شبکه های ویژه بی سیم منطبق با تغییر پذیری متفاوت و طرح های ترافیک ، این مقاله شیوه ای را برای تعویض از یک پروتکل به پروتکل دیگر به صورت پویا پیشنهاد می دهد ، در حالیکه مسیر یابی ادامه می یابد . با درج لایه نازک جدید ، قادر شدیم هر گره را در شبکه ویژه بی سیم درباره تعویض پروتکل از یکدیگر مطلع کنیم . برای اطمینان از اینکه مسیر یابی به خوبی کار می کند بعد از اینکه پروتکل تعویض شد، به ساختارهای داده های پروتکل مسیر یابی مقصد ، مقدار اولیه دادیم و اطلاعات قبلی مسی یابی برای ساختن جدول جدید مسی یابی دوباره استفاده کردیم . همچنین شیوه خود را تحت توپولوژی های متفاوت شبکه و الگوهای ترافیک را در شبکه های ایستا برای یادگیری امتحان کردیم چه در حالی که تعویض سریع بوده و چه در موقعی که تعویض متحمل خسارت بسیار زیادی شده باشد . پی بردیم تأخیر تعویض با طبیعت پروتکل مقصد و توپولوژی شبکه مرتبط است . همچنین پی بردیم که نسبت بسته کنترلی بعد از تعویض نزدیک به اجرای کنترل بدون تعویض است که نشانگر این است که روشمان خسارت زیادی را برای تعویض متحمل نمی شود .

1-مقدمه

شبکه ویژه موبایل (MANET) مجموعه ای از کامپیوترهای متحرک متصل از طریق سینک های بی سیم است. با همکاری بسته های مسیر یابی در میان گره ها، این گره ها می توانند بدون هر ساختاری، بایکدیگر ارتباط داشته باشند. بنابراین شبکه های ویژه اغلب برای استفاده در موقعیتهای اضطراری از قبیل محیطهای حادثه و کشمکشهای نظامی پیشنهاد می شود. مهم است که شبکه های ویژه باید به تغییرات توپولوژیکی شبکه و تقاضاهای ترافیک به صورت به یک روش مناسب واکنش دهند و پهناس باند درونی محدودیت های انرژی را رعایت کنند (24). چینی پروژه، عملکرد الگوریتم های مختلف مسیر یابی ویژه را مقایسه می کند (20)، (10)، (5)، (17). همه آنها پی بردند که هر الگوریتم مسیر یابی می تواند در شرایط مشخص بسته به حجم کار زمینه، ویژگیهای شبکه یا الگوی تغییر پذیری گره، کارایی بیشتری نسبت به بقیه داشته باشند.

گری و همکاران (10) چهار الگوریتم مختلف مسیر یابی را مقایسه کردند aodv (20)، odmrp (16)، aprl (15) و stara (11)، (12). مولفان از هر دو شبیه سازی و آزمایشات واقعی صفحه آزمایش استفاده کردند و پی بردند که تحت شرایط مختلف شبکه بی سیم، عملکرد وابسته، یکسان نبود. برای مثال نسبت تحویل پیغام ODMRP بهتر از نسبت در بیرون است در حالیکه AODV نسبت بالائی در تحویل پیغام در درون دارد (10) بروج و همکاران (5) DSDV، TORA، DSR و AODV را مقایسه کردند فهمیدند که خسارت مسیر یابی DSDV تقریباً با توجه به میزان تغییر پذیری ثابت بود، در حالیکه خسارت مسیر یابی

TORA ، DSR و AODV کاهش می یابد همانطور که میزان تغییر پذیری کاهش می باید . لی و همکاران (17) ، ODMRP ، AMROUT (4) ، CAMP (8) ، AMRIS (29) و طغیان را مقایسه کردند ، به این نتیجه رسیدند که در یک سناریوی موبایل ، پروتکل‌های چند مسیری (ODMRP) کارایی بیشتری نسبت به پروتکل‌های درختی (AODV) داشته باشند اما اشاره کردند که ODMRP روندی از افزایش سریع خسارت را با افزایش تعداد ارسال کننده ها نشان می دهد . ناندا (20) ، LAR ، MLAR ، AODV و AOMDV را در شبیه سازی وسیع در الگوهای تغییر پذیری در 20 و 30 مقایسه کرد و مزایای متمایزی را برای یک پروتکل بیش از دیگری در ترافیک متفاوت مربوط و شرایط تغییر پذیری به دست آورد .

پروتکل‌های مسیر یابی شبکه ویژه بی سیم معمولاً به دو گروه تقسیم می شوند : مسیر یابی کنش گرا ( جدول انجام شده ) و واکنشگر ( بنا به تقاضا ) (26) پروتکل‌های مسیر یابی کنش گرا مسیر ها را در حالت پیشرفته محاسبه می کنند ، در حالیکه پروتکل‌های مسیر یابی واکنش گرا مسیر ها را تنها موقع لزوم محاسبه می کنند . هر دو آنها مزایا و مضراتی دارند . بنابراین پروتکل‌های مسیر یابی هیبرید هر دو مد مسیر یابی کنش گرا و واکنش گرا پیشنهاد شده اند (13) ، (21) ، (23) . پروتکل‌های مسیر یابی منطقه ( ZRP ) (13) شبکه را به مناطقی در اندازه های متغیر تقسیم می کند . مسیر یابی درون منطقه از الگوریتم‌های کنش گرا استفاده می کند و مسیر

یابی بین مناطق از الگوریتم های واکنش گر استفاده می کند . الگوریتم های مسیر یابی هیبرید دیگری وجود دارد که الگوریتم های مسیر یابی کنش گرا و واکنش گر را از قبیل harp ( 21 ) و SHARP (23) ترکیب می کند . برای کاهش خسارت این روشهای هیبرید نزدیک گره ها ، دسته بندی شده و الگوریتمهای مسیر یابی کنش گرا را درون گروه ها استفاده می کنند و الگوریتم های مسیر یابی واکنش گر را بین گروه ها استفاده می کنند . چن و همکاران (6) مسی یابی تطابقی را با استفاده از کلاستد پیشنهاد دادند که توان عملیاتی را تا حد 80٪ بهبود می داد . بلدینگ رویر و همکاران (3) پروتکل های سلسله مراتبی را برای کاهش خسارت و بدست آوردن مقیاس پذیری بیشتر، پیشنهاد دادند . با این وجود چون تکنیک ها ، اطلاعات توپولوژیکی سطح بالایی را استفاده می کنند ، ممکن است که یک مسیر برای مقصد مطلوب نباشد و خود اطلاعات توپولوژیکی اضافی به حافظه زیادی نیاز دارد . هوبک و همکاران (14) ، الگوریتم مسیر یابی چند میسکی تطابقی را پیشنهاد می دهند . اجرا در لایه شبکه به مولفه آماری افزوده شد : آنها آمار خیر محلی را از طریق انتشار دوره های پیغام هلو (Hello message) به همسایه ها جمع کردند . روش آنها راندمان را بوسیله سویچینگ به پروتکل های متفاوت ، بهبود می دهد . با این وجود برای دستیابی به این راندمان ، مولفه های بسیاری را برای الگوریتم مسی یابی معرفی کردند که پیچیدگی الگوریتم را افزایش داد . جنبه عمومی تلاشهای قبلی ، اجازه دادن الگوریتم به مسیر یابی برای وفق دادن بوسیله ترکیب پروتکل های چندگانه است

چون برای مطرح شدن با پروتکل مسسیر یابی سخت است که برای همه موقعیت ها ، بهتر است . شیوه ما ، انتخاب یکی از سه پروتکل مسسیر ایبی موجود بصورت پویا نسبت به ساختن الگوریتم مسسیر یابی تطابقی جدید است ، هدفمان دستیابی به عملکرد بهتر از طریق سویچینگ پویا به بهترین پروتکل بر طبق شرایط شبکه بیسیم جاری است . در این مقاله روی مکانیسمی برای سویچینگ پروتکلها نسبت به سیاستی برای انتخاب موقع سویچ کردن تمرکز می کنیم . مخصوصاً مکانیسمی را توسعه می دهیم و برای شبکه گره ها ارزیابی می کنیم تا برای پروتکل مسسیر یابی جدید ، سویچ کنیم . برای ساده کردن روش مرکب خود ، فرض کردیم که پیش از این ، این ویژگی های پروتکلی های موجود می دانیم و برای انتخاب بهترین پروتکل مسسیر یابی بر اساس الگوی ترافیک شبکه جاری ، چند مکانیسم وجود دارد . برای مثال ، روش هوبک را برای جمع کردن آمار درباره ترافیک شبکه جاری ، تشخیص الگوی ترافیک و سپس انتخاب پروتکل کنش گرا و واکنش گر برطبق آن ، می توانیم استفاده کنیم . در شبکه های ویژه ، هر گره هردورا به عنوان میزبان و مسسیر یاب عمل می کند . همچنین دو واژه ((الگوریتم مسسیر یابی)) به طور تبادل پذیر استفاده می کنیم . در بخش 2 ، سه الگوریتم مسسیر یابی متفاوتی را معرفی می کنیم ، AODV ، QDMRP و APRL . تفاوت بین این سه پروتکل را توصیف می کنیم و عملکرد آنها را مقایسه می کنیم . همچنین SWAN ، شیبه سازی موقع اجرای آزمایشات را معرفی می کنیم . در بخش 3 ، روشی را برای سویچ میان سه الگوریتم مسسیر یابی پیشنهاد می دهیم و موضوعات

اجرای این روش را بحث می کنیم . در بخش 4 نصب آزمایشی خود را توضیح می دهیم در بخش 5 عملکرد این روش را مطالعه می کنیم و در بخش 6 مزایا را بحث می کنیم در بخش 7 مطالب را خلاصه و نتیجه گیری می کنیم .

پروتکل مسیریابی خود را روی شبیه ساز دارت ماوس Dart mouth را برای شبکه های ویژه بی سیم (swan) اجرا کردیم در حادثه موازی گسسته گرداننده شبیه ساز dassf ساخته می شود [v] که اجرای C++ ساختار ابتدایی مقیاس پذیر شبیه سازی (SSF) است [27] DASSF بویژه برای عملکرد بالا به هنگام شبیه سازی سیستم ارتباطات بزرگ بهینه ساخته می شود [18] چون DASSF قادر به شبیه سازی مدل شبکه است که هزاران گره را در بر می گیرد SWAN دو لایه از پروتکل 802/11 را اجرا می کند : شبه جلسه پروتکل برای لایه فیزیکی و جلسه پروتکل برای لایه MAC لایه های IP و ARP انتقال یافته از کد شبیه ساز SSFNET [27] را در بر می گیرد . ویژگی مناسب SWAN این است که می توانیم به طور پویا ، پشته پروتکل را با استفاده از زبان DML شکل دهیم . پته پروتکل کل سیستم ، در شکل 1 ، نشان داده شده که از پنج لایه تشکیل می شود . پروتکل های مسیریابی AODV ، ODMRP ، APRL در بالا ، بالای UDP هستند .

اجرای موجود AODV ، ODMRP و APRL را از پروژه اکت کام دارت ماویس

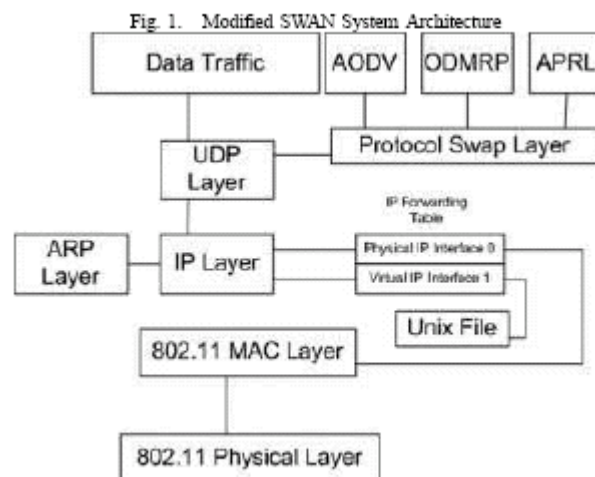
(Doortmouth Actcomm) استفاده کردیم [1]. هر سه پروتکل مسیر یابی در فضای کاربر روی

لیناکس Linux اجرا شدند و از تونل ip و سکوت های USP برای اجرای مسیر یابی آنها استفاده می کند.

تونل ip، وسیله شبکه مجازی است که فایل وسیله UNIX و رابط شبکه را وصل می کند. هر گره، نشانی

مجازی IP مربوط با رباط شبکه تونل و نشانی فیزیکی IP، مربوط با رباط شبکه واقعی در جدول ارسال IP

گره دارد (شکل 1).



در ابتدا، برنامه کاربردی بسته ها را با استفاده از نشانی مجازی IP گره مطلوب مقصد می فرستد سپس بسته ها

برای فایل وسیله UNIX از طریق تونل IP ارسال می شود. عد از آن، موتور مسیر یابی مجازی IP را به

نشانی مقصد فیزیکی IP تبدیل می کند و نشانی فیزیکی IP مسی بعدی را بر طبق جدول مسیر یابی آن پیدا می

کند و بسته ها را به پایین لایه IP می افزاید. این بسته ها با نشانی فیزیکی IP به جای رابط شبکه مجازی به رابط

شبکه واقعی ارسال می شود. بسته با نشانی مجازی اصلی در بسته IP نشانی داده شده به نشانی فیزیکی IP مسیر



بعدی در لایه IP پوشانیده می شود. در نتیجه، شبکه مجازی به شبکه فیزیکی تبدیل می شود. وقتی بسته ها می رسند، شبیه ساز موتور مسیر یابی را درباره این حادثه مطلع می کند و موتور مسیر یابی، بسته را باز می کند و نشانی مجازی را برای دیدن کنترل می کند، چه بسته به مقصد رسیده باشد یا برای ارسال دوباره نیاز داشته باشد. در نهایت، وقتی بسته در مقصد می رسد، شبیه ساز موتور مسیر یابی را آگاه می سازد و موتور مسیر یابی، بسته را به فایل وسیله UNIX برای تحویل به برنامه کاربردی می نویسد. سیستم می تواند برای هر دو شبیه سازی و نیز آزمایشات فیلد استفاده شود [10].

#### A - مسیر یابی بردار فاصله بنا به تقاضای ویژه (Aodv)

اجرای AODV اکت کام (ACTCOMM)، انشعابی از AODV پیشنهاد شده است که انتشار پیغام هلو Hello را می افزاید. این اجرا، قادر به انتقال و انتشار مسیر یابی است. بسته های کنترل، چهار نوع هستند: HELLO، RERR، PREQ، RREP. سه تای اولی با انتشار فرستاده می شود، در حالیکه RREP با انتقال فرستاده می شود.

#### B - پروتکل مسیر یابی تبدیل نوع چند گانه بر اساس تقاضا (ODMRP)

ODMRP ، یک پروتکل مسیر یابی تبدیل نوع چند گانه بر اساس تقاضا است . بسته های کنترل ، دو نوع هستند: سؤال پیوند و جواب پیوند . سؤال پیوند به وسیله انتشار فرستاده می شود و جواب پیوند با انتقال فرستاده می شود . سؤال و جواب پیوند ، هر دو مبدع و گروه تبدیل نوع چند گانه است . ODMRP از گروه های تبدیل نوع چند گانه برای حفظ اطلاعات عضو استفاده می کند . برای هر گره شناخته شده M در کل شبکه ، ODMRP گروه تبدیل نوع چند گانه را برای آن M حفظ می کند که ID گروه تبدیل نوع ، نشانی MS IP است . هر گره ODMRP ، علاوه بر جدول مسیر یابی ، دو ساختار اطلاعاتی دارد : جدول گروه تبدیل نوع چند گانه و کش پیام . جدول گروه تبدیل نوع چند گانه همه گروه های تبدیل نوع چند گانه را برای یک گره را در بر می گیرد . کش پیام برای کشف حلقه های مسیر یابی استفاده می شود . جدول گروه تبدیل نوع چند گانه دارای تاریخ انقضاء و اطلاعاتی است درباره اینکه چه مسیر را برای M می شناسد یا باید اطلاعات نشأت گرفته از M را دریافت کند . با اینکه ODMRP ، پروتکل تبدیل نوع چند گانه است ، از آن تنها به عنوان پروتکل انتقال استفاده می کنیم .

C- هر مسیر یابی راه بدون حلقه ها (APRL):

APRL ، پروتکل مسیر یابی کنش گرای انتقالی است [15] . دونوع بسته کنترل وجود دارد : Beacon و POVN . گره به طور دوره ای سیگنال ها (Beacon) را به همسایه هایش انتشار می دهد . هر سیگنال

(Beacon) اطلاعات مسیر شناخته شده بوسیله ارسال کننده را در بر می گیرد . بسته های مقصد پینگ (Ping) از طریق همسایه (PDVN) برای تأیید مسیر هایی استفاده می شود که گره در سیگنال ها (Beacon) دریافت می کند . براساس راه اندازی ، هر گره پیغام سیگنال (Beacon) رابه همسایه هایش انتشار می دهد ، تا جائیکه هر جدول مسیر یابی گره ها تنها مقصدهای همسایه هایش را در بر می گیرد. بعداز ارزش اولیه دادن به به جدول مسیر یابی به تنها اطلاعات همسایه اش ، هر گره جدول مسیر یابی خودش را به صورت دوره ای به همسایه اش انتشار می دهد . اگر هیچ مسیری برای مقصد مورد نیاز بسته وجود نداشته باشد ، بسته داده ها رها می شود . برخلاف AODV ، مکانیسم درخواست مسیر وجود ندارد .

### 3. اجرا

دراین بخش ، روش خود را برای ترکیب سه پروتکل متفاوت بحث می کنیم . به وضوح ، لایه جدیدی را بین پروتکل های مسیر یابی و لایه UDP (یا لایه معادل درچند ساختار دیگر) درج می کنیم . این لایه جدید را لایه تعویض پروتکل می نامیم . بنابراین ، تغییر در پروتکل برای لایه پایین تر (درمورد لایه UDP) ، شفاف است .

A - روش مرکب

به این دلیل که لایه جدیدی را بین لایه مسیر یابی و لایه UDP درج می کنیم ، هر بسته کنترل تولید شده با پروتکل های مسیر یابی از طریق لایه تعویض پروتکل جدا می شود که بسته با اطلاعات اضافی یعنی نوع پروتکل و عدد دوره

(epoch number) پوشانیده می شود (شکل 2).

Fig. 2. Packet Format (top = old; bottom = new)

MAC	IP	UDP	Control Packet
-----	----	-----	----------------

MAC	IP	UDP	Epoch Num.	Control Packet
-----	----	-----	------------	----------------

این دو فیلد اضافی ، نوع پروتکل و تازگی پروتکل را به ترتیب مشخص می کند . برای هر بسته کنترل دریافت شده ، ابتدا اطلاعات اضافی را در لایه تعویض پروتکل را بررسی می کنیم و سپس بسته کنترل را به پروتکل مسیر یابی مناسب ارسال می کنیم ( موضوعی برای جزئیات بحث شده در پایین )

به علت درج لایه تعویض پروتکل نشان داده شده در شکل 1 ، نوع پروتکل و عدد دوره برای لایه پروتکل مسی یابی شفاف هستند . مزیت این لایه در این است که تنها مجبوریم رابط را با لایه تعویض پروتکل تغییر دهیم میتوانیم بخش مسیر یابی کدهای پروتکل مسیر یابی موجود را دوباره استفاده کنیم . همچنین همه کدها را برای تعویض پروتکل ها در لایه تعویض پروتکل بسته بندی می کنیم . زیت دیگر این است که روش مرکب ، خسارت کمی به همراه دارد ، به این خاطر که (1) دو فیلد تنها 4 بیت هستند که برای جلوگیری از ابهام نوشتار محیطی هنوز کوچک است . چون یک بسته کنترل از هدر MAC ، یک هدر IP ، یک هدر UOP و

بدنه بسته کنترل تشکیل یافته ، دو فیلد اضافی ، پهنای باند اضافی را استفاده نمی کنند . (2) تنها بسته های کنترل با نوع پروتکل و عدد دوره پوشانیده می شود ، در حالیکه بسته های داده ها همانند قبل باقی می ماند . (3) در طول زمان اجرا ، تناه جدول مسیر یابی پروتکل رایج حفظ می شود و دیگر جدولهای مسیر یابی مرکب پروتکل ، خالی هستند . بنابراین ، روش مرکب برای جدولهای مسیر یابی زیاد ، حافظه اضافی را اشغال نمی کند . (4) تا کنون ، اجرای لایه تعویض پروتکل با لایه های تعویض پروتکل دیگر اتصال مجازی برقرار نمی کند که به این مفهوم است که این روش هر بسته جدید کنترل را اختراع نمی کند . (5) ما توانستیم مؤلفه نمایشگر ترافیک در این لایه اضافه کنیم . برای مثال ، اگر یک گره پی برد که نسبت تقاضاهای مسیر بالاتر از حد معمول است ، ممکن است تصمیم بگیرد به پروتکل مسیر یابی دیگر تعویض شود . این موضوع فراتر از حوزه این مقاله است ولی می خواهیم این موضوع را در بخشی در کار بعدی بحث کنیم .

B - مشکلاتی که باید حل کنیم :

برای اجرای روش مرکب که می توانیم از یک پروتکل به پروتکل دیگری تعویض شود ، سه مشکل برای حل کردن وجود دارد :

(1) تعویض چه زمانی و به چه نحوی و به دست چه کسی مشخص می شود ؟

(2) تصمیم تعویض به چه نحوی به تمام گره ها منتقل می شود ؟

3) چطور هر گره، جدول های درونی خود را وفق می دهد تا تعویض انجام شود؟

راه حل کامل برای این مشکل، خارج از حوزه این مقاله است. به سادگی فرض می کنیم که یک گره اصلی می تواند تعویض پروتکل را ره بیندازد و همه گره ها را درباره تعویض مطلع کند. فراتر از حوزه این مقاله است تا تعیین کنیم چه زمانی باید تعویض رخ دهد یا برای کدام پروتکل رخ دهد.

C - چطور یک تعویض صورت می گیرد؟

گره اصلی، تصمیمش را از طریق ارسال بسته کنترل با نوع پروتکل و عدد دوره به همسایه هایش ارسال می کند. گره اصلی عدد دوره را افزایش می دهد و نوع پروتکل هر زمان که برای تعویض تعیین می شود، تغییر می یابد. بعد از اینکه همسایه ها به پروتکل جدید تغییر می یابد، تمام بسته های کنترل آتی آنها، این فیلد نوع پروتکل و عدد دوره را استفاده خواهد کرد، بنابراین خبرها منتشر می شود. با این وجود، هدر لایه تعویض پروتکل را به بسته های داده ها نمی افزایشیم چون بسته های داده ها برای دانستن اینکه پروتکل مسیریابی برای یافتن مسیر مقصد استفاده می شود، نیازی ندارد. حتی اگر دو گره، پروتکل های مسیریابی متفاوتی را استفاده می کنند، هنوز می توانند بسته های داده ها را به یکدیگر ارسال کنند و شبکه می تواند ارسال بسته ها را ادامه دهند، حتی زمانی که تعویض در حال انجام است. مکانیسم برای تعویض پروتکل به هر گرهی برای ثبت مفهوم خودش از نوع پروتکل محلی و عدد دوره نیاز دارد. سپس، هدر لایه تعویض پروتکل از بسته ای پیام

دریافتی مقایسه می کند تا تعیین کند که دوره جدید رخ داده است و بنابراین زمان سویچ برای پروتکل جدید است. دو حالت قابل توجه جود دارد:

حالت اول: عدد پروتکل دریافت شده همانند عدد پروتکل محلی است. حالت IQ: عدد دوره دریافت شده، کمتر از عدد دوره محلی است، گره بسته را رد می کند. Ib: عدد دوره یکسان است، بسته را پردازش می کند. IC: عدد دوره دریافت شده بزرگتر از عدد دوره محلی است، گره عدد دوره محلی خود را به روز می کند تا عدد دوره دریافت شود و بسته را پردازش می کند.

حالت دوم: عدد پروتکل دریافت شده از عدد پروتکل محلی متفاوت است. حال a 2: عدد دوره دریافت شده کمتر یا برابر با عدد دوره محلی آن است. گره بسته را رد می کند. b 2: عدد دوره دریافت شده بزرگتر از عدد دوره محلی است. گره عدد دوره محلی خود را به روز می کند تا عدد دوره دریافت شود، پروتکل دریافت شده را تعویض می کند سپس بسته را پردازش می کند.

D - برای تعویض، لازم است تا به جدول مسیر یابی پروتکل مقصد جدید و ساختارهای داده های دیگر از طریق استفاده از آنها از پروتکل رایج مقدار اولیه دهیم. اولین هدف موقع تغییر پروتکلها، ساختن جدول مسیر یابی برای پروتکل های جدید و دادن مقدار اولیه تا حد ممکن از طریق اطلاعاتی در جدول مسیر یابی برای پروتکل قدیمی است. به همه شش حالت مختلف برای تعویض توجه می کنیم:

(a) AODV به ODMRP یا APRL (b) ODMRP به AODV یا APRL و (c) APRL به AODV یا ODMRP.

E- استفاده مجدد از ورودی های جدول مسیر یابی قبلی :

برای گرفتن مزایای اطلاعات مسیر یابی پروتکل ، ورودی ها در جدول مسیر یابی قبلی دوباره استفاده می کنیم . با این وجود ، ورودی ها در جدول مسیر یابی AODV ، ODMRP و APRL متفاوت هستند که تلاشمان را برای کپی ورودی ها بین پروتکل های مسیر یابی پیچیده تر می کنند . هر فیلد مشابه دو ورودی را کپی می کنیم و مقدار معمولی را برای فیلدهای متفاوت انتخاب می کنیم . بسیار مهم است که دقت کنیم که AODV ، ODMRP و APRL ، همه دو فیلد اساسی برای مسیر یابی دارند : نشانی مقصد IP و نشانی مسیر بعدی IP . این دو فیلد ، مسیر بعدی را برای ارسال بسته ها به مقصد تعیین می کنند . چون تمام این پروتکل های مسیر یابی از این دو فیلد برای تعیین هر مسیر استفاده می شود ، برای کپی این دو آدرس IP از ورودی جدول مسیر یابی قبلی به ورودی جدول مسیر یابی جدید ، صحیح است . فیلدهای دیگر برای تعیین وضعیت رایج مسیر ها به کار می رود . AODV ، ODMRP و APRL وضعیت متفاوت مسیرها را برای مسیر یابی حفظ می کند ،



بنابراین ممکن است برای استفاده مجدد آنها در پروتکل جدید، درست نباشند. اما می توانیم به دقت مقدار پیش فرض درستی را انتخاب کنیم. در اینجا، جزئیات را به دلیل کمبود فضا حذف می کنیم اما آنها را در یک کار تحقیقی [30] حاضر می کنیم و همچنین درستی و موانع این مقدارهای پیش فرضی را توضیح می دهیم. یک مزیت اصلی استفاده مجدد ورودی جدول مسیر ایبی قبلی این است که قادریم بع از تعویض، حذف اکثر هزینه پتانسیل یک تعویض، از مسیر قبلی استفاده کنیم.

#### F – ساختارهای داده های اصلی

برای اجرای تعویض، نه تنها جدول مسیر یابی بلکه ساختارهای ویژه داده های مربوط هر پروتکل را نیز تغییر می دهد. هر ساختار داده را به ترتیب بحث می کنیم. لیست پیشگام AODV: ساختار داده ها، تمام گره های جهت بالا را در بر می گیرد که از خود گره به طرف همان مقصد استفاده می کند. اگر گره تعیین کند که هر یک از لینکهایش شکسته است، به عنوان یک اشاره، بسته RERP را به همسایه هایی می فرستد که در لیست پیشگام آن هستند. وقتی که با AODV تعویض می کنیم، ترک لیست پیشگام خالی بی خطر است چون این ساختار داده ها موقعی که گره بعداً به RREQ فرستاده می شوند، دوباره ساخته می شوند.

صف بسته AODV: صفهای گره منبع هر بسته داده ها که هنوز هستند به صفهای بسته و مقصد فرستاده می شوند. وقتی که ما از AODV به پروتکل دیگری تعویض می کنیم، بسته ها را در این صفها رد می کنیم و از

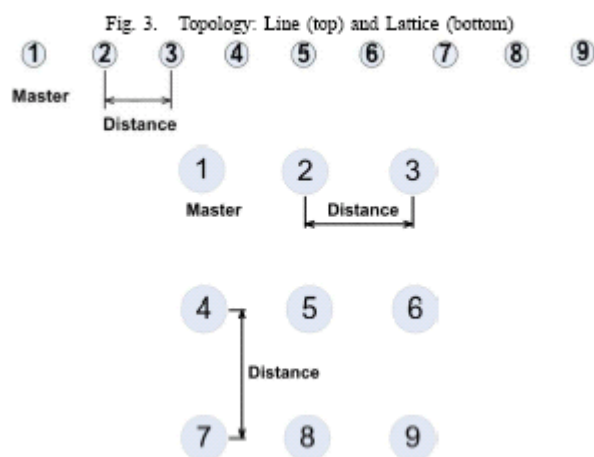
دست می روند. فرض کردیم که برخی از مکانیسم های دیگر (از قبیل TCP) تشخیص می دهد که این بسته ها به مقصدشان نرسیدند و داده ها دوباره فرستاده می شوند. صف بسته ، ساختار بی نظیری از داده های AODV است ، پروتکل های دیگر صفی برای بسته داده ها ندارند .

اگر ما برای AODV تعویض کنیم ، می توانیم به سادگی صفهای خالی را بسته بسازیم .

کش بسته AODV RREQ : این ساختار داده ها اخیراً برای ذخیره بسته های RREQ جهت پرهیز از حلقه ها استفاده می شود . وقتی که برای ODMRP تعویض می کنیم ممکن است به عنوان خالی ساخته شود و وقتی از ODMRP تعویض کنیم ، ممکن است رد شده باشد .

جدول گروه تبدیل نوع چندگانه : این ساختار داده برای حفظ لیست گروه های تبدیل نوع چندگانه در جایی استفاده می شود که این گروه ، یک عضو است و موقع دریافت سؤال پیوند بررسی می شود . اگر این گروه در گروه تبدیل نوع چندگانه است ، پس باید بسته سؤال پیوند را بپذیرد و جواب پیوند را برگرداند . ODMRP باید دوباره جدول گروه تبدیل نوع چندگانه از طریق سؤال های پیوند را موقع تعویض به ODMRP بسازد . این ساختار داده ها ممکن است موقع تعویض به ODMRP ساخته شود و ممکن است موقع تعویض از ODMRP رد شود . APRL ساختارهای داده زیادی ندارد . بنابراین چیز زیادی برای انجام دادن موقع تعویض به یا از APRL وجود ندارد .

هدف ما، ارزیابی خسارت (از لحاظ زمان و ترافیک) به سبب تعویض پروتکل است. شبکه ایستا را انتخاب می‌کنیم که به این معنی است که همه گره‌ها برای موقعیت معین از پیش تنظیم شود و در طول آزمایشات حرکت نمی‌کند. مسافت موثر انتقال رادیوی گره تشبیه شده، 73 M پروتکل را برای 200 ثانیه اجرا کردیم و تعویض در ثانیه 100 رخ داد. دو نوع از توپولوژی شبکه انتخاب کردیم (شکل 3):

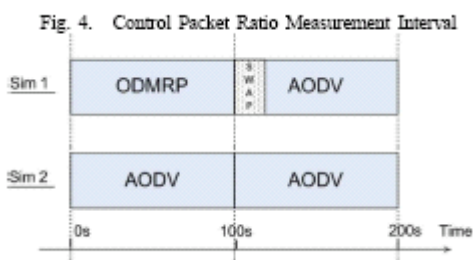


شبکه خطی و شبکه مربعی.

دو اندازه شبکه را انتخاب کردیم: 4 گره و 49 گره. دوسرعت ترافیک را انتخاب کردیم. بسته داده‌های 1 نشأت گرفته از هر گره در هر ثانیه یا بسته داده‌های 1 نشأت گرفته از هر گره در 5 ثانیه. هر مقصد بسته داده‌ها از میان بقیه گره‌ها به طور یکسان انتخاب می‌شود. هر ترکیب پارامتر، 5 بار اجرا کردیم، هر بار به یک شکل تصادفی SWAN را جستجو می‌کند. نتایج را گزارش می‌دهیم.

A – عملکرد روش مرکب خود را با AODV ساده ، APRL و ODMRP مقایسه می کنیم . از دو متریک استفاده کردیم : زمانی برای کامل کردن تعویض پروتکل و نسبت بسته های کنترل هر بسته داده فرستاده شده از لایه UOP ،

متریک اول : زمانی برای تکمیل تعویض پروتکل . زمان تعویض وقتی شروع می شود که گره اصلی تقسیم به تعویض کردن می گیرد و وقتی پلین می یابد که همه گرهها در شبکه عدد پروتکلی محلی خود و عدد دوره محلی را به روز می کنند . بنابراین متریک ، زمان پایان تعویض و شروع تعویض است . این متریک ، تأخیر تعویض را اندازه گیری می کند .



متریک دوم : نسبت بسته های کنترل تبدیل نوع تکی و چندگانه هر بسته داده فرستاده شده از لایه UOP یعنی نسبت بسته کنترل . این متریک در ارزیابی رانندگی پروتکل مقصد بعد از تعویض به ما کمک می کند .

AODV چهار بسته کنترل دارد : HELLO، RREQ، RREP، RERR .RREP تبدیل نوع تکی

است و بقیه تبدیل نوع چندگانه هستند . APRL دو بسته کنترل دارد : BEACON، PDVN . PDVN

تبدیل نوع تکی است و BEACON تبدیل نوع چندگانه است . ODMRP دو بسته کنترل دارد : سؤال پیوند

و جواب پیوند . جواب پیوند تبدیل نوع تکی است و سؤال پیوند ، تبدیل نوع چندگانه است . در تمامی موارد ، نسبت بسته کنترل تعداد بسته های کنترل (تبدیل نوع تکی و چندگانه ) تقسیم شده از طریق تعداد بسته های داده فرستاده شده از لایه UOP است . نسبت بسته های کنترل را در سه فاصله زمانی با استفاده از دو شبیه سازی اندازه گیری می کنیم : 1) فاصله زمانی بعد از تعویض پروتکل مقصد . 2) نیمه اول فاصله زمانی شبیه سازی مختلف تنها در پروتکل مقصد . 3) نیمه دوم فاصله زمانی همان شبیه سازی پروتکل مقصد . برای مثال در شکل 4 ، شبیه سازی 1 تعویضی را از ODMRP به AODV با شروع در  $t = 100s$  انجام می دهد . بنابراین AODV پروتکل مقصدمان است .

TABLE I  
TEST CONFIGURATIONS

Config	Layout	Nodes	Dist.	Master node's neighbors
1	Line	9	20m	3
2	Line	49	20m	3
3	Square	9	25m	8
4	Square	49	30m	8

TABLE II  
ASSOCIATION WITH NETWORK CONNECTIVITY

Config	Layout	Nodes	Dist.	Max Swap Latency
1	Line	9	20m	10.004 sec
2	Line	49	20m	35.048 sec
3	Square	9	25m	1.813 sec
4	Square	49	30m	6.014 sec

شبیه سازی 2 ، یک شبیه سازی تنها از پروتکل مقصد برای 200 ثانیه است . بنابراین نسبت بسته کنترل را برای سه فاصله زمانی زیر مقایسه می کنیم : 1) پروتکل مقصد بعد از تعویض از شبیه سازی 1 (زمانی که گره ها ،

تعویض را تا پایان شبیه سازی در  $t = 200s$  خاتمه می دهند. (2) پروتکل مقصد برای 100 ثانیه اول از سیم

(3,2sim) پروتکل مقصد برای 100 ثانیه دوم از سیم (sim)2.

## B – محیط

همانطور که در جدول 1 نشان داده شده است ، چهار پیکربندی را انتخاب کردیم . با توجه به شکل 3 و

فراخوانی فاصله مؤثر ارتباط (73m) ، چندین گره در حوزه هر گره وجود دارد که گره اصلی را در بر می

گیرد . اگر چه تمامی گره ها ، به طور مستقیم یا غیر مستقیم به یکدیگر متصل شدند ، می توانیم در پیکربندی 3

بینیم که تمامی گره ها درون حوزه ارسال همدیگر متصل شدند ، اما در پیکربندی های دیگر ، ارتباط مسیری

چند گانه نیاز است .

## 5- نتایج شبیه سازی

از متریک هایی استفاده کردیم که در بالا برای اندازه گیری راندمان تعویض برای پروتکل مقصد داده شده ،

تعریف کردیم . حداکثر یا متوسط تأخیر تعویض را برای همان پروتکل مقصد از دو منبع مشخص می کنیم .

برای مثال در جدول 3 ، متوسط تأخیر تعویض را از ODMRP به AODV و APRL به AODV به عنوان

تأخیر تعویض برای AODV استفاده می کنیم .

## A – تأخیر تعویض

1) ارتباط با اتصال پذیری شبکه ها : جدول 2 و 3 هر دو نشان می دهد که تأخیر تعویض مربوط به اتصال پذیری شبکه برای هر نوع تعویض است . بالاترین اتصال پذیری (پیکربندی 3) هترین تأخیر تعویض را دارد و کمترین اتصال پذیری (پیکربندی 2) بدترین تأخیر را دارد .

2) ارتباط با ترافیک شبکه : جدول 4 نشان می دهد برای AODV و APRL ، تأخیر تعویض مشابه با حجم کار ترافیک کم و سنگین بود . برای ODMRP ، تأخیر تعویض ترافیک سنگین حدوداً دوبرابر سریعتر از تأخیر ترافیک کم است . چون ODMRP ، پروتکل مسیر یابی واکنش دار است ، تنها موقع نیاز سؤال پیوند را می فرستد .

TABLE III  
AVERAGE SWAP LATENCY (s) WITH DIFFERENT NETWORK TOPOLOGIES

Configuration	To AODV	To ODMRP	To APRL
9 node Line	0.988	2.620	7.518
49 node Line	3.945	4.6146	31.045
9 node Square	0.050	1.233	0.012
49 node Square	2.493	2.006	11.021

TABLE IV  
AVERAGE SWAP LATENCY (s) WITH DIFFERENT TRAFFIC PATTERNS

	To AODV	To ODMRP	To APRL
Avg. Latency (Low Traffic)	1.788	1.435	12.029
Avg. Latency (High Traffic)	1.950	3.801	12.769

بنابراین الگوی ترافیک شلوغ تر ، ترافیک کنترل بیشتری تولید می کند و بنابراین خبرها درباره تعویض پخش می شود . اما AODV و APRL هر دو بصورت دوره ای پیغام را به همسایه هایش انتشار می کند ، بنابراین فاصله زمانی تعویض . بیشتر به فاصله زمانی انتشار بستگی دارد تا به بار ترافیک .

3) ارتباط با پروتکل مقصد : جدول 5 نشان می دهد که AODV و ODMRP ، تعویض را به سرعت تکمیل می کند در حالیکه APRL نسبتاً آرام است . بعد از تعویض ، ODMRP نیاز دارد تا بسته های سؤال پیوند را برای حفظ اطلاعات عضو گروه تبدیل نوع چندگانه انتشار دهد . به همین نحو ، AODV نیاز دارد تا اگر هیچ مسیری برای مقصد در جدول مسیر یابی بعد از تعویض نباشد ، PREQ انتشار می یابد . اما APRL ، اگر نتواند اطلاعات مسیر را در جدول مسیر یابی آن پیدا نکند ، افت می کند .

سؤال مسیر انتشار بسته به AODV و ODMRP به سرعت تعویض می کند . در جدول 2 ، می توانیم ببینیم که اتصال پذیری بالای پیکربندی های مربعی (ردیف 3 و 4) ، AODV و APRL به سرعت تعویض می شود . این به این خاطر است که هر دوی آنها به صورت دوره ای ، پیغام را به همسایه هایش انتشار می کنند .

TABLE V  
AVERAGE SWAP LATENCY (s) OVER ALL TESTED CONFIGURATIONS

	To AODV	To ODMRP	To APRL
Average Latency	1.8692	2.6186	12.3995

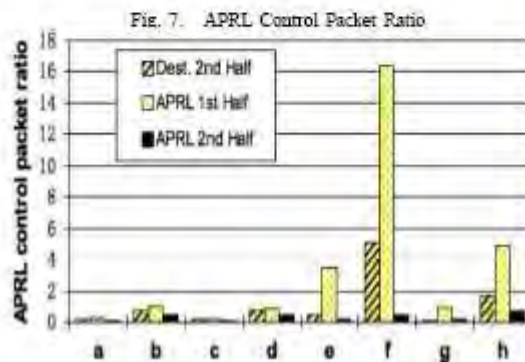
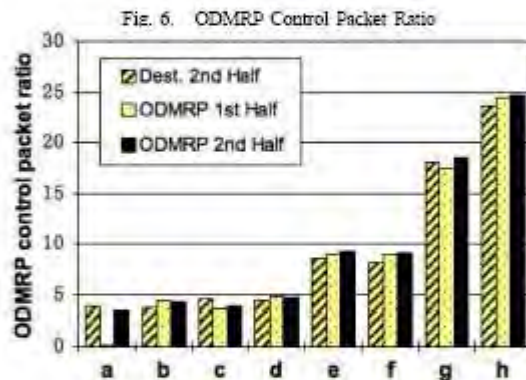
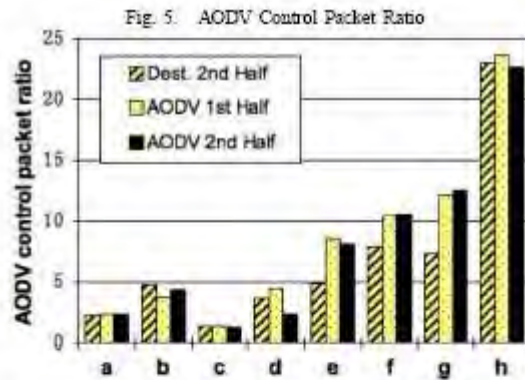
TABLE VI  
MEASURED SWAP LATENCY (s) WITH THE DESTINATION PROTOCOL  
OVER ALL TESTED CONFIGURATIONS

Config. Format= Number of nodes/Layout/Traffic-pattern  
Sq = Square; Ln = Line; Lo= Low Traffic; Hi= High Traffic

No.	Config.	To AODV	To ODMRP	To APRL
a	9/Ln/Hi	0.928	1.645	5.032
b	9/Ln/Lo	1.048	3.595	10.004
c	9/Sq/Hi	0.098	0.652	0.009
d	9/Sq/Lo	0.001	1.813	0.014
e	49/Ln/Hi	1.235	2.593	27.043
f	49/Ln/Lo	6.655	6.635	35.048
g	49/Sq/Hi	4.890	0.849	16.032
h	49/Sq/Lo	0.095	3.162	6.010



همچنین می توانیم در جدول 6 ببینیم که AODV و ODMRP تعویض خود را حتی در اتصال پذیری کم شبکه های خطی تکمیل کند . اما زمان تعویض APRL با توپولوژی شبکه به شدت مرتبط است . برای مثال محدوده تأخیر تعویض AODV از 0/001 تا 6/665 ثانیه بود و محدود ODMRP از 0/652 تا 6/635 ثانیه بود . محدوده تأخیر تعویض APRL از 0/009 تا 35/048 ثانیه بود ، با این وجود به خاطر اینکه APRL تنها برای همسایه های خود بصورت دوره ای ، سیگنال ها (beacon) را انتشار می دهد . بنابراین تأخیر تعویض نسبت به الگوی ترافیک همانند AODV یا ODMRP به دوره این انتشار بستگی دارد .



## B – نسبت بسته کنترل

در شکل‌های 5، 6 و 7، نسبت بسته های کنترل 8 نوع پیکربندی های شبکه را مطابق با همان مورد لیست شده در ستون های او 2 جدول 6 نشان می دهیم . برای هر پیکربندی و نوع تعویض ، می توانیم ببینیم که نسبت بسته های کنترل بعد از تعویض (اولین میله در هر سه گروه) در اکثر حالتها ، بزرگترین نسبت هر گروه نبود . حتی

اگر نسبت بسته های کنترل بعد از تعویض ، بزرگترین نسبت هر گروه بود ، واریانس بین سه میله ، کم بود . بعد از تعویض در بیشتر حالت ها پروتکل مسیر یابی مقصد ، تقریباً به صورت شفاف اجرا شد حتی اگر بدون تعویض باشد و بسته های داده ها به موفقیت و با خسارت کم کنترل مسیر یابی شد . برای APRL ، میله سوم همیشه کوچک هستند چون APRL ، بسته های کنترل زیادی را به یک شبکه ایستای فرستد ، مسیرها تثبیت شده است و تمامی مقصدها ، قابل دسترس هستند .

## 6- بحث

تأخیر تعویض با اتصال پذیری شبکه ، ترافیک شبکه و خصوصیات پروتکل مقصد مرتبط است . اولاً پی بردیم که تأخیر تعویض به اتصال پذیری شبکه بستگی دارد ، چون اخبار تعویض برای پیمایش کردن ، مسیر های کمتری دارد . همچنین فهمیدیم که جمع کار ترافیک ، تأخیر تعویض پروتکل های مسیر یابی واکنش گر را مانند ODMRP تحت تأثیر قرار داد . در نهایت نیز تأخیر تعویض به خصوصیات ترافیک داده ها بستگی دارد تا بسته های کنترل را تولید کند و بنابراین اخبار تعویض را انتشار می دهد ، پروتکل های کنش گرا برای پخش اخبار به انتشار دوره ای بستگی دارد . اگر یک پروتکل ، مسیر یابی را بدون طغیان اجرا می کند ، تأخیر تعویض طولانی بود (به ویژه در شبکه هایی با ارتباط کم) . در این مورد ، ممکن است گرهی به برگرداندن پیغام کنترل

خالی نیاز داشته باشد تا ارسال کننده را درباره دوره جدید و پروتکل مسیر یابی البته در صورت دریافت هر بسته کنترل قدیمی از ارسال کننده ، مطلع کند .

B – تعویض ، بسته های کنترل زیادی را موجب نمی شود .

همانطور که نتایج نشان می دهد ، نسبت بسته کنترل بعد از تعویض کمتر یا نزدیک به نسبت بسته کنترل از اجرای یک پروتکل بدون تعویض بود . اولاً تعویض ، بسته های کنترل زیادی را برای پراکندن اطلاعات تعویض یا ساختن دوباره جدولها نیازی ندارد . ثانیاً به این دلیل که مقدار اولیه ای را با استفاده از مسیر های قدیمی به جدول مسیر یابی جدید می دهیم ، بسته های کمی را از سؤال مسیر می فرستیم . این وضعیت تنها وقتی منطقی است که در شبکه های ایستا یا شبکه هایی با تغییر پذیری کم باشد . در شبکه هایی با تغییر پذیری بالا ، ترافیک کنترل زیادی برای ساختن مجدد مسیری به مقصد داشته باشد و بسته های داده زیادی را از دست می دهد . با این وجود ، اگر تعویض رخ نداده باشد ، همان منطقی خواهد بود . بنابراین معتقدیم که روشمان به طور مؤثری شبکه را بدون استفاده از هیچ نوع بسته ای ، استفاده مجدد اطلاعات جدول مسیر یابی در جای ممکن و نه در افزایش بی نهایت ترافیک کنترل بعد از تعویض ، از یک پروتکل به دیگری انتقال می دهد .

C – روش بی نظیر

هوبک و همکاران پروتکل مسیر یابی چند حالتی انطباقی را برای شبکه های ویژه پیشنهاد داد [14] اما نتایج عملکرد را فراهم نمی کند. روش انطباقی آنها باروش مرکب ما مشابه می باشد: هر دو می خواهند تا به صورت پویا به پروتکل دیگری بر اساس شرایط رایج شبکه تعویض کند ولی سه تفاوت عمده وجود دارد. 1) روش انطباقی آنها نوع جدیدی از بسته کنترل را به پروتکل های موجود معرفی کرد که به صورت دوره ای انتشار یافت. روشی ماهیچ پیام جدیدی را به پروتکل های موجود معرفی نکرد. بنابراین، برای ترکیب پروتکل های زیاد در صورت لزوم، نسبتاً آسان است. از سوی دیگر، اگر بخواهیم تا پروتکل های  $n$  را ترکیب کنیم، به طراحی مبدل های جدول مسیر یابی  $n(n-1)$  نیازمندیم.

2) در روش آنها، پروتکل های متفاوتی، همان جدول مسیر یابی را به اشتراک می گذارند، نیاز همه پروتکل ها برای وفق دادن فرمت جدید جدول مسیر یابی دوباره اجرا می شود. هر گره نیز برای حفظ تراک اتصال پذیری و حالت های همسایه ها (کنش گرا و واکنش گر)، یک جدول همسایه دارد. در روش ما، هر یک از پروتکل های مختلف، جدول مسیر یابی خودشان را حفظ می کنند و موقع تعویض پروتکل ها، جدولها را انتقال می دهیم. بنابراین به تغییر فرمت جدول مسیر یابی نیاز نداریم و جدول همسایه جدیدی را معرفی می کنیم.

3- ما واقعاً این ایده را SWAN اجرا کرده ایم و می توانیم از این کد برای هر مورد شبیه سازی ها و آزمایش های فیلد واقعی استفاده کنیم . در شبیه سازی ها ، عملکرد الگوریتم مسیر یابی را برای تعویض بین سه پروتکل تحلیل کرده ایم .

#### 7- خلاصه

ما روشی را برای ترکیب AODV ، ODMRP و APRL توصیف می کنیم به طوری که می توانیم از یک پروتکل به دیگری تعویض می کنیم . برای هر جفت پروتکل ، مشخص می کنیم چطور مقدار اولیه ای را برای ساختار داده هر پروتکل از ورودی های پروتکل دیگر بدهیم . برای اندازه گیری عملکرد و توپولوژی های مختلف تشبیه شده شبکه و شرایط با استفاده از SWAN ، دو متریک پیشنهاد دادیم . نتایج نشان می دهد که زمان برای تکمیل تعویض پروتکل به خصوصیات پروتکلی که می خواهیم تعویض کنیم ، توپولوژی شبکه و ترافیک شبکه بستگی دارد . روش مرکب ما برای شبکه هایی با اتصال کم به کندی تعویض می شود و برای پروتکل هایی بدون طغیان (مانند APRL) نیز آهسته تعویض می شود ولی در تمام حالت های دیگر مؤثر بود . در روش مرکب ما از نقطه نظر مهندسی نرم افزار ، می توانیم کد منبع پروتکل مسیر یابی را از طریق درج لایه جدید برای تحصیل تعویض بدون تغییر اجرای پروتکل موجود ، دوباره استفاده کنیم .

#### 8- کارهای بعدی

توجه کردیم که نتایج ما بر اساس شبیه سازی هاست . با اینکه با شبیه سازی دقت کردیم ، نتایج باید در طی آزمایشات واقعی رسیدگی می شد . برای راحتی ، ما از شبکه های ایستا برای اجرای شبیه سازی خود استفاده کنیم . با این وجود ، این شبکه های ایستا نتوانستند آزمایش کنند که روشمان برای شبکه هایی با تغییر پذیری بالا مؤثر می باشد . تغییر دیگر این است که آیا باید اجازه دهیم لایه تعویض پروتکل یک بسته خالی را تنها برای مطلع کردن همسایه هایش برای تعویض انتشار یابد . این انتشار باید زمان تکمیل تعویض را از طریق افزایش سرعت انتشار اخبار درباره تعویض کاهش دهد . این امر ممکن است برای پروتکل هایی که به صورت دوره ای انتشار نمی یابند ، مؤثر باشد . همچنین توانستیم برخی از فیلدها را در آن هدر بسته خالی بیفزاییم تا آمار را در کنار نوع پروتکل و عدد دوره حمل کنیم . با این وجود ، این فیلدها ، پیچیدگی لایه تعویض پروتکل را بیشتر می کنند و احتمالاً خسارت را نیز افزایش دهند .

منابع :

- 1- لی گرلا ، طراحی ، اجرا و ارزیابی عملکرد پروتکل مسیر یابی تبدیل نوع چندگانه بنا به تقاضا در شبکه های بی سیم چند مسیری . 2000 ص 77 - 70
- 2- بلدینگ رویر . سلسله مراتب های چند سطحی برای مسیر یابی ویژه مقیاس پذیر ، شبکه های بی سیم . 2003 ص 461 - 478
- 3- بومایا ، لیو . پروتکل مسیر یابی تبدیل نوع چندگانه ویژه . 1998
- 4- بورچ ، مالتز ، جانسون ، هو و جتچووا . مقایسه عملکرد پروتکل های مسیر یابی شبکه ویژه بی سیم چند مسیری . 1998 ص 85 - 97
- 5- چن ، سیتمن . الگوریتم منطقه ای برای گروه بندی شبکه های ویژه 2003 ص 305 - 3220
- 6- دارتماس ( Dartmouth ssf )
- 7- پروژه اکت کام ( Actcomm )
- 8- مادروگا . پروتکل چند مسیری . 1999 ص 1380 - 1394
- 9- گرلا . تحلیل عملکرد تبدیل نوع تکی ODMRP در صفحه آزمایش شبکه ویژه موبایل . 2000 ص 148 - 150
- 10- گری ، کوتز ، نیوپارت . مقایسه بیرون آزمایشی چهار الگوریتم مسیر یابی ویژه . 2004



- 11 - گ.پتا و کومار . سیستم و ترافیک بسته به الگوریتم مسیر یابی انطباقی بریا شبکه های ویژه . 1997  
ص 270-283
- 12 - گوپتا . تحلیل طراحی و عملکرد شبکه بی سیم . 2000
- 13- پییرلمان. عملکرد برنامه کنترل سؤال برای پروتکل مسیریابی منطقه 2001 ص 421-438
- 14- هوبک، دیستر . مسیر یابی چند حالتی انطباقی در شبکه های ویژه موبایل . 2004  
ص 107-117
- 15- کارپ کونگ . کشف پویای همسایه و حلقه 1998 .
- 16- گرلا . پروتکل مسیر یابی تبدیل نوع چند گانه بنا به تقاضا در شبکه های موبایل بی سیم چند مسیری .  
2000
- 17- گرلا ، لی ، باگرو دیا. مقایسه عملکرد پروتکل های تبدیل نوع چند گانه بی سیم ویژه 2000 ص 574  
- 565
- 18 - ینکل . راهنمای کاربرد . 2001
- 19- یوان ، یفکل ، گری ، کوتز ، فلیپ . تصدیق شبیه سازی با استفاده از اجرای مستقیم پروتکل های مسیر  
یابی بی سیم . 2004 ص 7- 16
- 20- سومندرا ناندا و روبرت . MLAR در 2D و 3D . 2006

- 21- نوید ، بونت . پروتکل مسیر یابی ویژه هیبرید . 2001
- 22- پرکینز ، رویر ، داس . مسیر یابی ویژه بردار مسافت بنا به تقاضا . 1999 ص 100-90
- 23- سیور. پروتکل مسیر یابی انطباقی هیبرید برای شبکه های ویژه موبایل . 2003 ص 314 – 303
- 24- کارسون ، ماکر . شبکه ویژه موبایل 1999
- 25- پرکینز ، بلدینگ رویر . مسیر یابی ویژه بردار مسافت بنا به تقاضا . 2003
- 26- رویر . مرور پروتکل های مسیر یابی رایج برای شبکه های ویژه بی سیم موبایل . 1999 ص 55 – 46
- 27- ساختار ابتدایی شبیه سازی مقیاس پذیر .
- 28- شبیه ساز شبکه های ویژه بی سیم .
- 29- تای . استفاده از پروتکل مسیر یابی ویژه تبدیل نوع چندگانه . 1998
- 30- جیانگ . روش مرکب مسیر یابی برای شبکه های ویژه بی سیم .

این مقاله، از سری مقالات ترجمه شده رایگان سایت ترجمه فا میباشد که با فرمت PDF در اختیار شما عزیزان قرار گرفته است. در صورت تمایل میتوانید با کلیک بر روی دکمه های زیر از سایر مقالات نیز استفاده نمایید:

لیست مقالات ترجمه شده ✓

لیست مقالات ترجمه شده رایگان ✓

لیست جدیدترین مقالات انگلیسی ISI ✓

سایت ترجمه فا ؛ مرجع جدیدترین مقالات ترجمه شده از نشریات معتبر خارجی