# بهبو پروتکل مسیر یابی AODV در برابر حمله سیاه چاله


## چکیده

در دهه‌های اخیر، شبکه های بیسیم موردی (Wireless Ad Hoc Networks) توجه بسیاری را در زمینه تحقیقات محاسبات سیار و بیسیم بخود جلب کرده‌اند. این شبکه‌ها در برابر تعدادی تهدیدات امنیتی آسیب پذیر می باشند که میتواند به شدت کارایی آنها را تحت تاثیر قرار دهد. این مشکل در زمانی که شبکه برای یک کاربرد حساس داشته باشد، حیاتی‌تر و مهم میشود. شبکه بیسم موردی روشی خاصی به منظور دفاع در برابر حملات ندارد، بنابراین به سادگی در دسترس کاربران شبکه های تهدید کننده و گره های مخرب است. در حضور گره های مخرب، از چالش های مهم در این شبکه، طراحی راه حل های امنیتی ایمن می باشد که می تواند آن را از حملات مختلف مسیریابی محافظت نماید. در این مقاله به تجزیه و تحلیل شبکه های بیسیم موردی و همچنین حمله سیاه چاله و پروتکل مسیر یابی aodv پرداخته میشود و سپس روشی برای مسیریابی AODV جهت دفاع در برابر حمله سیه چاله ارائه میشود تا کارایی ا شبکه را بهبود بخشد و در اخر روش ارائه شده به همراه AODV در شبیه ساز شبکه در یک سناریو متغییر شبیه سای شده وبر اساس نتایج بدست امده از شبیه سازی انجام شده پروتکل بهینه معرفی میگردد.



کلمات کلیدی: شبکه های بیسم، پروتکل مسیریابی؛ تهدید امنیتی، حمله سیاه چاله، شبیه سازی

**مقدمه**

شبکه های بیسیم موردی [3]به شبکه های موقت گفته می شود که برای یک منظور خاص به وجود می آیند. در واقع شبکه های بی سیم هستند که گره های آن متحرک می باشند. تفاوت عمده شبکه های بیسم موردی با شبکه های معمول بی سیم 802.11 در این است که در شبکه های بیسیم موردی مجموعه ای از گره های متحرک بی سیم بدون هیچ زیرساختار مرکزی، نقطه دسترسی و یا ایستگاه پایه برای ارسال اطلاعات بی سیم در بازه ای مشخص به یکدیگر وصل می شوند . این نوع شبکه ها بیشتر در مقابل حمله قرار می گیرند حمله های از قبیل خمله سیه چاله؛ کرم چاله، که قرار گرفتن در مقابل این حملات، از دست دادن اظلاعات و کاهش کارایی شبکه را بدنیال دارد.

در حمله ی سیاه چاله مهاجم تلاش می کند تا بیشتر داده های شبکه را جمع آوری کند و سپس شبکه را از کار بیندازد. کارهای زیادی برای بهبود امنیت شبکه های بیسیم در برابر حملات سیاه چاله انجام شده است. در مقاله [1] شاخص هدایت بسته به عنوان روشی برای تشخیص گره های سیاه چاله و چاله خاکستری ارائه شده است که در این مقاله شاخص هدایت بسته به عنوان پارامتر اعتماد برای تشخیص گره های مخرب ارائه شده است. این شاخص براساس نوع عملکرد گره ها در عملیات هدایت بسته های داده، گره های مخرب را شناسایی می کند در مقاله [2] دو بهبود برای امنیت در مقابل حملات داخلی ارائه شده است. روش اول ارسال بسته های داده از روی مسیرهای مستقل است. این روش تضمین می کند که اگر یک پیام از دست برود(دراپ شود)، مسیر دیگر داده را به صورت موفق تحویل می دهد. روشی دیگر که در این مقاله [2] آمده انتخاب دینامیکی گام بعدی از میان یک سری از گره های داوطب است که این روش باعث تغییر مداوم معماری شبکه می شود و این تغییر مداوم باعث می شود که نتوان هیچ پارامتر کیفیت سرویسی را تضمین کرد.

## پروتکل مسیریابی aodv

یک پروتکل مسیریابی مبتنبی بر درخواست است[4]، که به کامپیوترهای سیار، یا گره‌ها، برای انتقال پیام-ها در میان همسایه‌هایشان اجازه می‌دهد تا با هم به طور مستقیم ارتباط برقرار کنند. این پروتکل مانند، تمام پروتکل های پیش فعال تنها وقتی مسیری مورد نیاز باشد عملیات یافتن مسیر انجام می‌گیرد و البته وقتی که

مسیر یافته شد، تا زمانی که مورد احتیاج باشد آن مسیر در جدول مسیر یابی ذخیره شده، باقی می‌ماند و پس از آن دیگر نگه داشته نشده و برای دفعهٔ بعد باید دوباره یافته شود. AODV، تضمین من کند که مسیرها شامل حلقه نباشند یعنی این پروتکل عاری از حلقه است و برای پیدا کردن کوتاه‌ترین مسیر ممکن سعی می‌کند. همچنین AODV قادر به تغییرات دستی در مسیرها است و اگر یک خطا وجود داشت می‌تواند مسیرهای جدید خلق کند.

این پروتکل سعی می‌کند به سرعت با شرایط خطوط پویا هماهنگ شود و حجم کم پردازش و حافظه مورد نیاز از خواص این الگوریتم می‌باشد. این پروتکل از شمارهٔ ترتیبی مقصد برای اطمینان از عدم ایجاد حلقه‌ها استفاده می‌کند و همچنین مشکل شمردن تا بینهایت را که در پروتکل کلاسیک بردار فاصله موجود بود، حل می‌کند. در AODV هر گره دارای شمارهٔ ترتیبی مخصوص به خود است که به طور یکنواخت افزایش می‌یابد. این شمارهٔ وقتی افزایش می‌یابد که گرهٔ مربوطه متوجه تغییری در توپولوژی شبکه گردد.AODV قابلیت مهم دیگری نیز داراست و آن قابل استفاده بودن این پروتکل در هر سه نوع ارتباطات تک‌پخشی، چند-پخشی و انتشاری می‌باشد [5].

## روش پیشنهادی

روش پیشنهادی سعی بر این است تا بتوان با توجه به رفتار گره ها در شبکه در مورد خرابکار بودن یک گره تصمیم گیری کرد . اصول روش پیشنهادی به صورت زیر است:

۱. ثبت اطلاعات مربوط به فعالیت گره ها که شامل موارد زیر می باشد:
   - تعداد داده های ارسالی به گره همسایه
   - تعداد داده های دریافتی از یک گره همسایه
   - تعداد پاسخ های (reply) دریافتی از یک گره همسایه
۲. ارسال بسته درخواست نظرات همسایه ها در مورد یک گره همسایه که بسته RREP را ارسال کرده است
۳. دریافت اطلاعات ثبت شده در گره های همسایه در مورد گره فرستنده بسته RREP

۴. بررسی اطلاعات دریافتی و اعلام نظر در مورد خرابکار بودن گره
۵. ارسال یک بسته خطر برای قرنطینه کردن گره خرابکار
۶. حذف گره های داخل قرنطینه در فرآیند مسیریابی

در روش پیشنهادی هر گره در شبکه دارای ساختمان داده های زیر می باشد:

۱. هر گره دارای یک جدول مربوط به همسایه ها و رفتارهای آنها می باشد . هر مدخل این جدول مشخص می کند که گره همسایه با Id مشخص، چند بسته داده به این گره ارسال کرده است، چند بسته RREP به این گره ارسال کرده است و گره مورد نظر به گره همسایه چند بسته داده تحویل داده است.
۲. هر گره دارای لیستی از گره هایی است که در قرنطینه می باشند و باید این گره ها را از فرآیند مسیریابی حذف کرد.

الگوریتم پیشنهادی بر روی پروتکل AODV پیاده سازی شده است و برای انجام عملیات های خود از چندین بسته جدید استفاده می کند که عبارتند از:

- بسته درخواست اطلاعات در مورد یک گره
- بسته اطلاعات گره های همسایه در مورد گره مورد سوال

بسته اعلام خطر: این بسته شامل گره هایی است که خرابکار شناخته شده اند و باید در لیست قرنطینه گره ها قرار گیرند. بسته اعلام خطر در کل شبکه پخش می شود

## شبیه سازی

هدف اصلی از شبیه‌سازی تحلیل عملکرد پروتکل مسیر یابیAODV در برابر حمله سیاه چاله با روش پیشنهادی است. شبیه‌سازی توسط شبیه‌ساز NS2[7] انجام شده است.. در شبیه‌سازی ، یک شبکه با تعداد گره های متغییر در نظر گرفتیم (15,20,25,30,35,40,45,50) ،گره هایی که به صورت تصادفی در یک ناحیه ۱۰۰۰*۱۰۰۰ متر مربع و عملیات بیش از ۱000 ثانیه قرار داده شده-اند، در نظر می‌گیریم. اجراهای چندگانه و متعدد با تعداد گره متفاوت محاسبه شده و از داده‌های جمع‌آوری شده میانگین گرفته شده است. برای محاسبه عملکرد پروتکل مسیریابی مختلف ما به هر

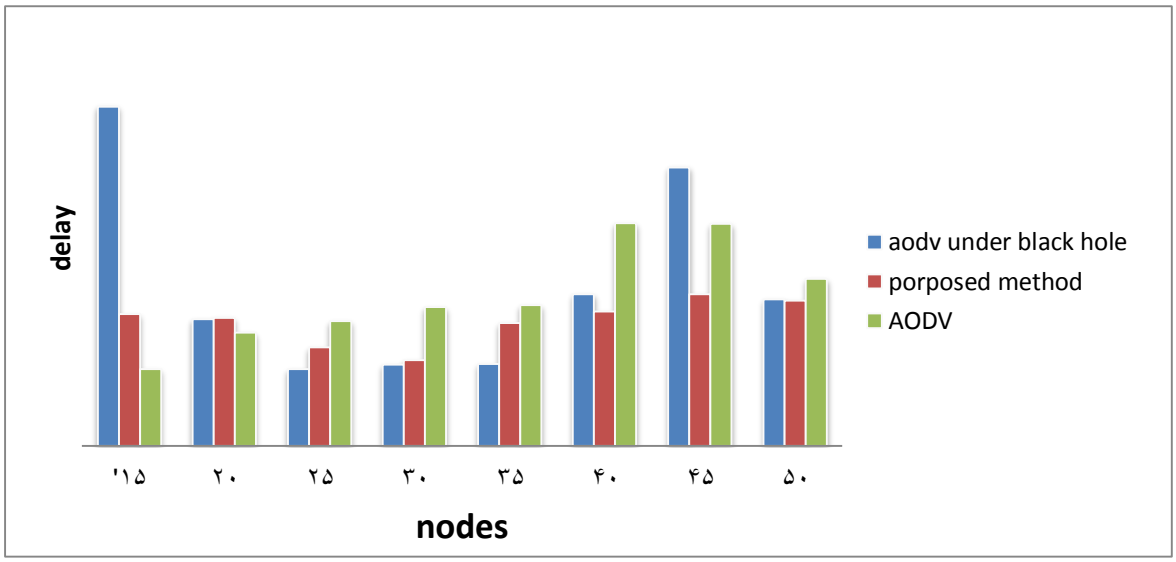
دو معیار کیفی و کمی نیاز داریم. برخی از معیارهای کمی که به منظور مقایسه عملکرد پروتکل‌های مسیریابی مختلف استفاده می‌شود عبارتند از

- نسبت تحویل بسته، میانگین تأخیر انتها به انتها و توان عملیاتی

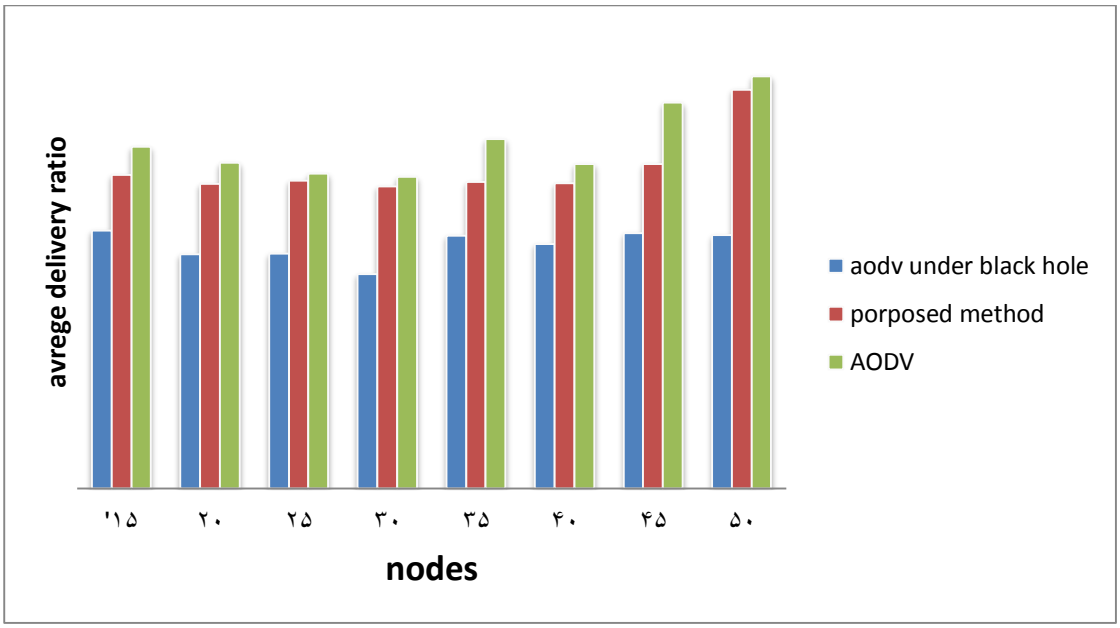
جدول پارمترهای شبیه سازی

| نام | مقدار |
|---|---|
| محیط شبیه سازی | ۱۰۰۰*۱۰۰۰ |
| زمان شبیه سازی | ۱۰۰۰s |
| پروتکل مسیر یابی | AODV |
| نوع صف | DropTail |
| استاندارد MAC | ۸۰۲,۱۱ |
| تعداد گره | 15,20,25,30,35,40,45,50 |
| پهنای یاند | ۱Mbps |
| محدوده انتقال | ۲۵۵m |

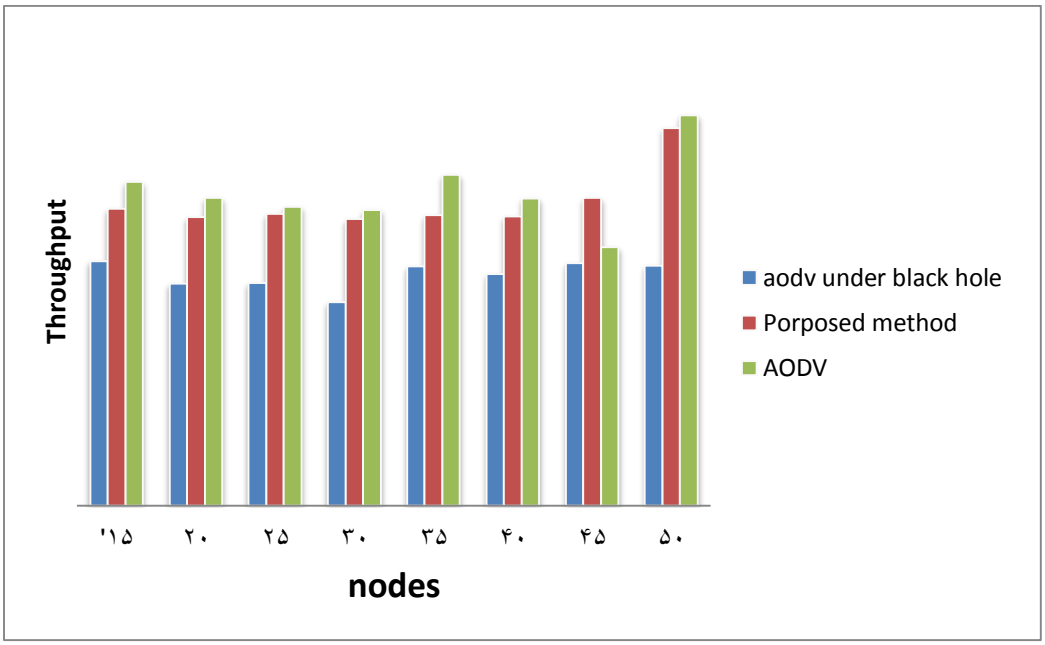
## نتایج شبیه سازی




شکل ۱- تاخیر انتها به انتها نسبت به تعداد گره ها




شکل-۲- نرخ تحویل بسته به نسبت تعداد گره ها




شکل-۳- توان عملیاتی به نسبت تعداد گره ها

## نتیجه گیری

با کمک شبیه ساز شبکه NS-2 روش پیشنهادی و پروتکل مسیر یابی AODV در یک سناریو مورد ارزیابی و مقایسه قرار گرفته شد و بر اساس نتایج بدست امده از شبیه سازی و تجزیه تحلیل متریک های ذکر شده در فوق، نتیجه گیری میشود که روش پیشنهادی به دلیل شناسایی گره های مخرب و همچنین انتخاب مسیر بهتر و بهینه طبق روش ارائه شده در این مقاله از کارایی بهتر و بیشتری نسبت به پرو تکل AODV تحت حمله دارد.

منابع

[1] H. Terpsichori, N. Velivasaki, P. Karkazis, V. Theodore, and V. Zahariadis, "Trust-aware and link-reliable routing metric composition for wireless sensor networks," presented at the TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, 2012

[2] T. Tsao, R. Alexander, M. Dohler, V. Daza, and A. Lozano, "A Security Framework for Routing over Low Power and Lossy Networks," presented at the IETF Requirement Draft for Routing over Low Power and Lossy Networks

[3]. S. Corson and J. Macker, Mobile ad hoc networking (MANET)" Routing protocol performance issues and evaluation considerations

[4]. Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routingprotocols for mobile ad hoc networks. Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia,2003

[5] C. Perkins, E. Belding-Royer, and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, July2003.