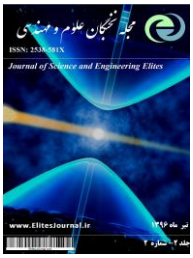
مجله نخبگان علوم و مهندسی
Journal of Science and Engineering Elites
ISSN 2538-581X
جلد ۲- شماره ۲- سال ۱۳۹۶
www.ElitesJournal.ir



ارائه الگوریتمی مبتنی بر بسته تله جهت تشخیص حمله کرم چاله در شبکه های موردی از طریق پروتکل مسیریابی AODV

حمید باسره[1*]، مسعود مرادخانی[2]

۱- کارشناسی ارشد مهندسی نرم افزار، دانشگاه آزاد اسلامی واحد ایلام

۲- عضو هیئت علمی گروه مهندسی برق ، دانشگاه آزاد اسلامی واحد ایلام

*hamid.basereh20@gmail.com

ارسال: اردیبهشت ماه ۹۶ پذیرش: تیر ماه ۹۶

چکیده

شبکه‌های موردی متحرک شامل مجموعه‌ای از گره‌های بیسیم هستند که بدون داشتن هیچ‌گونه زیرساخت و مدیریت مرکزی، می‌توانند آزادانه و تنها از طریق فرکانس های رادیویی با یکدیگر در ارتباط باشند. این شبکه ها به علت گره پذیری باز و ساختار آسیب پذیری که دارند، عموما از لحاظ امنیتی مورد تهدید قرار می گرند. وجود انواع متعددی از حملات در این نوع از شبکه ها ، آنها را با مشکلات و چالش های فراوانی رو به رو کرده که می توان از حمله کرم چاله (Worm Hole) به عنوان یکی از مهمترین این حملات نام برد. در این پژوهش، الگوریتمی جهت تشخیص نفوذ و مقابله با این نوع از حمله در شبکه های مذکور و بر اساس پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا[1] ارائه شده است. این الگوریتم ابتدا همکاری های پرتکرار هرگره با سایر گره های شبکه را تحلیل و موارد بالای ۵۰ درصد همکاری میان دو گره خاص را نشانه گذاری و سپس با ارسال بسته های تله واقعی البته با سربار کم، آنها را مورد ارزیابی و امتحان مجدد قرار داده و از این طریق گره های همکار کرم چاله که قصد دارند با ایجاد یک تونل مجازی پنهان و دزدین بسته ها، در حقیقت شبکه را دور بزنند شناسایی و شبکه از وجود آنها ایزوله خواهد شد. شبیه سازی ایده پیشنهادی بهینگی پارامترهایی نظیر نرخ تحویل بسته ها، نرخ اتلاف بسته ها و تاخیر انتها به انتها در زمان های مختلف اجرا شدن یک شبکه موردی را اثبات می کند.

کلمات کلیدی: شبکه های موردی متحرک، حمله کرم چاله، پروتکل مسیریابیAODV، بسته تله، تشخیص نفوذ.

۱. مقدمه

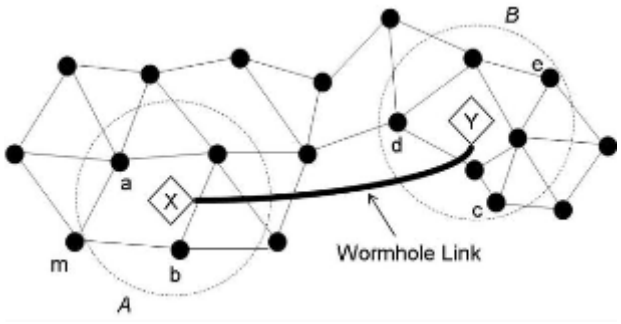
شبکه‌های موردی متحرک بیسیم در واقع نوعی از شبکه‌های ادهاک هستند که گره‌ها در آن ضمن حرکت کردن به صورت پویا که همین موضوع گاهی امنیت آن ها را به مخاطره می اندازد، هم نقش روتر و هم میزبان را بر عهده داشته و در حالی که دارای هزینه‌های نگهداری و تعمیر پایین‌تری نسبت به سایر شبکه‌ها می‌باشند، گره‌های فعال در این نوع از شبکه‌ها از طریق امواج رادیویی با یکدیگر ارتباط برقرار می‌کنند. باید گفت طراحی پروتکل‌های مسیریابی امن برای MANET[2] کار چندان آسانی نخواهد بود چرا که پهنای باند، ظرفیت پردازش پردازنده‌ها و حافظه و انرژی هر گره بسیار محدود می‌باشد [۱ و ۲].

[1] Ad-Hoc On-Demand Distance Vector
[2] Mobile Ad-Hoc Network

موضوع امنیت در واقع مهم‌ترین نگرانی استفاده کنندگان MANET می‌باشد. برخی از مهم‌ترین مشکلات این نوع شبکه‌ها را می‌توان تغییر مداوم توپولوژی به صورت پویا، ورودی پذیری آسان برای گره‌های جدید، عدم وجود الگوریتم دفاعی مشخص، محیط بیسیم ناامن، عدم وجود نقطه مرکزی جهت کنترل شبکه و محدود بودن توان منبع تغذیه هر گره عنوان کرد [۳ و ۴]. شبکه‌های موردی به سبب ساختار خود دارای حملات متعددی بوده که می توان از حمله کرم چاله به عنوان یکی از مهمترین و در عین حال متفاوت ترین این حملات نام برد.

۱.۱. حمله کرم چاله در شبکه‌های موردی متحرک

در این نوع از حملات در شبکه‌های موردی دو گره مخاصم و همکار به صورت همزمان به شبکه وارد می‌شوند. گره شماره یک معمولاً وظیفه پاسخگویی به مبدأ جهت اعلام نزدیک ترین مسیر به مقصد آن هم از طریق خود را بر عهده دارد و این در شرایطی است که امکان یا عدم امکان ارسال عبور بسته از طریق این گره هرگز ملاک سنجش توسط منبعی که بسته در اختیار دارد نخواهد بود.گره منبع با توجه به به اعلام نزدیک‌ترین مسیر توسط گره مخاصم اول و بدون توجه به پاسخ‌های سایر گره‌های سالم موجود در شبکه که فاصله‌ی واقعی خود تا مقصد را اعلام کردند به گره مخاصم اعتماد کرده و بسته را در اختیار او قرار می‌دهد. میان گره مخاصم اول و گره مخاصم دوم (همکار) پیش از جلب رضایت منبع توسط گره اول با ارسال یک سیگنال رادیویی، یک تونل ارتباطی مجازی جهت جریان عادی حرکت پیام‌ها و نشان دادن در همسایگی قرار داشتن آن دو گره ایجاد خواهد شد [۵].



شکل ۱- حمله کرم چاله در شبکه های موردی

گره اول پس از جلب رضایت و دریافت بسته از منبع و بر مبنای اصول حمله‌ای که ماهیت آن ها را ایجاد و شکل داده است، بسته‌ها را بدون توجه به اصول همکاری با همسایگانی که در مسیر آن گره تا مقصد وجود دارند، به طور مستقیم و بدون بر جای گذاشتن هیچ گونه رد و اثری به طرف گره مخاصم همکار ارسال کرده و از طریق این تونل مجازی غیر قانونی ایجاد شده، ضمن دزدی آشکار بسته‌های در حال عبور، شبکه و کارکرد آن را نیز دور زده و فریب خواهند داد [۶]. کرم چاله در واقع یکی از حملات بسیار مشهوری است که مختص به شبکه‌های موردی می‌باشد. اساس این حمله بر طراحی یک اتصال کوتاه در بستر توپولوژی شبکه توسط دو گره همکار اما مخاصم استوار می‌باشد [۷].

۲.۱. پیشینه تحقیق

در ادامه تحقیق به ذکر و توضیح مواردی از الگوریتم ها، پروتکل‌ها و پیشنهادات توصیفی در جهت کشف و برخورد با حملات کرم چاله در شبکه‌های موردی خواهیم پرداخت. روش‌هایی که در ادامه توضیح داده خواهند شد، بر گرفته از مقالات به چاپ رسیده شده در طی سالیان اخیر و در باره ی همین موضوع می باشد که به ذکر منابع تمامی آنها نیز اشاره خواهد شد.

ارائه روشی با موضوعیت قلاده‌های زمانی و مکانی جهت تشخیص حمله کرم چاله که در آن سعی شده است با ذخیره سازی موقعیت گره مبدأ و همچنین نگهداری زمان ارسال بسته و نیز ثبت موقعیت گیرنده بسته و زمان دریافت توسط آن، با آنالیز زمان مربوط به مبادله بسته و همچنین تطبیق با میانگین زمانی و مکانی از قبل پیش‌بینی شده، برای تشخیص حمله مذکور اقدام شود [۸].

ارائه ایده آنتن های جهت‌دار آن هم با فرض اینکه تمام گره‌های موجود در شبکه دارای آنتن‌های تراز شده باشند و یک کلید محرمانه بین هر آنتن با سیار آنتن‌ها به اشتراک گذاشته شود. در این روش لیستی از همسایگان امن هر گره تعیین و در صورتی که هرگره بدون همکاری بایکی ازهمسایگانش بسته راتامسیری نامعلوم ازخود دور کند،حمله کرم چاله تشخیص داده خواهدشد [۹].

ارائه ایده تشخیص حمله کرم چاله با عنوان بررسی گام‌های انتها به انتها. در این ایده تعداد گام‌های منطقی بین فرستنده و گیرنده تخمین زده شده و از گره واسط اول خواسته می‌شود که پس از عبور دادن بسته از خود، شماره شناسایی منحصر به فرد خود را به آن الحاق کرده و این روند را از گره پس از خود نیز درخواست کند و چون در حمله کرم چاله معمولا گیرنده، بسته را تنها در اختیار گره مخاصم و همکار خودش در هر جا از شبکه قرار می‌دهد، در صورت عدم همکاری بر مبنای قوانین ارائه شده و درج نشدن شماره منحصر به فرد گره مخاصم بر روی بسته، حمله کرم چاله به شبکه تشخیص داده خواهد شد[۱۰].

ارائه پروتکل با نام WHOP که با هدف اصلاح پروتکل AODV طراحی شده است. این روش به (سگ تازی) نیز معروف بوده که با تعقیب بسته‌ها و تحلیل شمارش متفاوت HOP بین همسایه ها، حمله کرم چاله را تشخیص می‌دهد [۱۱].

یک رویکرد پیشنهادی بر اساس پروتکل DSDV ، که هدف تشخیص لینک های مشکوک از طریق بررسی تغییرات در جدول مسیریابی را دنبال می‌کند [۱۲].

در این ایده از گره‌ای که خود را نزدیک ترین مسیر به مقصد معرفی می کند، خواسته می‌شود که قبل از دریافت بسته اعلام کند که پس قصد دارد پس از خود بسته را به کدام همسایه اش تحویل دهد تا روند ارسال بسته از طریق آن ادامه یابد. بدیهی است در صورت اعلام گره پس از خود توسط گره‌ای که اعلام آمادگی خود را به اطلاع گره منبع رسانده است، صحت ادعای او مورد بررسی و سپس بسته در اختیارش قرار خواهد گرفت. در اینجا اگر عملکردی خلاف هر آنچه به گره منبع اعلام شده بود صورت گیرد حمله به شبکه تشخیص داده خواهد شد. طبیعی است این روش برای شناسایی گره‌های مخاصمی که اصطلاحاً یک بار مصرف بوده و پس از دریافت و دزدیدن بسته قصد دارند شبکه را ترک کنند چندان کار آمد نبوده و طبق معمول حداقل یک بار دزدیده شدن بسته در این شبکه‌ها اتفاق خواهد افتاد [۱۳].

در این ایده ، مسیریابی بسته‌های ارسال شده مطرح و پیشنهاد شد که با ایجاد حساسیت بر روی مسیر ارسال بسته از ابتدا تا انتها و همچنین تحلیل چگونگی چرخش بسته میان گره‌های همسایه، امکان تشخیص و شناسایی حمله کرم چاله افزایش پیدا کند [۱۴].

در این مقاله ضمن آنالیز تعداد زیادی از ایده های ارائه شده در زمینه تشخیص نفوذ حملات کرم چاله از ابتدا تا آن زمان، عنوان شد که تشخیص حملات کرم چاله در ابتدا هرگز امکان‌پذیر نخواهد بود چرا که شبکه‌های موردی به ذاته دارای گره پذیری باز می‌باشند و پیشنهاد این بود که ماهیت شبکه‌های ادهاک مورد تغییر و تقویت قرار گیرد [۵].

ارائه یک روش ترکیبی پویا که در آن با آنالیز لحظه‌ای عملکرد تمام گره‌های دریافت کننده بسته و با شرط آنکه تعداد همکاری های هر گره با حداقل یکی از همسایگانش به صفر نرسد. حمله کرم چاله تشخیص داده خواهد شد. بدیهی است گره‌های مخاصم برای عدم شناسایی و نیز عدم الصاق شناسه منحصر به فرد خود به بسته‌های در حال عبور در بعضی موارد حتی یک بار نیز با همسایگان خود همکاری نخواهد داشت و همین موضوع امکان شناسایی مشکوک بودن فعالیت‌های آن‌ها را ممکن می‌کند[۶].

۳.۱. ایده پیشنهادی

حمله ی کرم چاله یکی از این حملات می باشد. با توجه به مطالبی که در بخش های قبلی توضیح داده شد، در این حمله گره مخرب سعی می کند با به انحراف کشاندن جریان مسیریابی، جهت ارسال بسته ها، مسیر عبوری از خود را کوتاه نشان داده و سپس با کمک یک شبکه خصوصی بین خود و گره مخرب دیگری(همکار) بسته را ارسال کند. حمله کرم چاله در حقیقت از این طریق جریان ارسال داده ها را مختل کرده و مانع از رسیدن صحیح بسته ها به مقصد خواهد شد. اساس روش پیشنهادی ارائه شده در این تحقیق هم بر این گونه خصیصه متمرکز بوده و سعی شده است تا با در نظر گرفتن اینگونه رفتار ها، گره های مخرب حمله کرم چاله شناسایی و به سایر گره ها معرفی شوند.

۲. روش پیشنهادی شامل چند فاز زیر می باشد

۱- بررسی ماهیت تمامی گره های فعال موجود و استخراج همکاری های پر تکرار(گره های کاندید)

۲- ارسال بسته های تله به گره های کاندید و برسی سلامت سنجی آنها

۳- معرفی گره های مخرب به سایر گره های سالم و ایزوله کردن آنها

۱.۲. فاز اول

بررسی ماهیت فعالیتی تمامی گره های موجود در شبکه و شناسایی همکاری های پر تکرار میان دو گره به گونه ای که ارتباط هر کدام از گره ها با تمامی همسایگانش مورد آنالیز قرار گیرد.سپس همکاری های پر تکراری که از یک آستانه ی منطقی معین عبور کرده اند انتخاب و در لیست بررسی مجدد قرار داده می شوند. در فاز مذکور همکاری های بالای ۵۰ درصد هر گره با سایر گره های شبکه شناسایی و در یک جدول به نام Black List مجازی قرار میگیرند. یعنی مشخص می شود که کدام گره ها بیش از ۵۰ درصد ورودی و خروجی هایشان تنها با یک گره مشخص مبادله می شود. در اینجا و با توجه به فاصله دوگره همکار از هم میتوان مشخص کرد که چه تعداد از گره های دوتایی شبکه با یکدیگر ارتباط کامل داشته و به عبور مسیر از طریق همسایگان خود بی تفاوت هستند.

هدف از شناسایی این نوع گره ها ناشی از خصیصه مشترک بین تمام گره های مخرب است که همگی به نحوی سعی خواهند کرد تا با به انحراف کشاندن فرایند مسیریابی، خود را در میان جریان های ارسال بسته ها قرار داده و مانع از رسیدن صحیح بسته ها به مقصد گردند.

فرایند شناسایی گره های کاندید در این فاز شامل مراحل زیر می باشد:

۱- گره IDS به عنوان یک گره فرستنده ظاهر شده و چندین پیام کشف مسیر RREQ را با مبدا یکسان و مقصدهای متفاوت و به صورت چندپخشی و به جهت کشف مسیرهای متفاوت به تمام گره های در دسترس خود ارسال کرده و منتظر پیام های پاسخ RREP همه مسیرها می ماند.

۲- با اتمام مدت زمان مجاز شبکه و بررسی پیام های پاسخ رسیده و به کمک الگوریتم های انتخاب کوتاه ترین مسیر، مسیر بهینه برای تمام مسیرهای درخواست شده انتخاب می شود (مانند S1,S2 ..... SN). بدیهی است که دلیل انتخاب کوتاه ترین مسیر ، وقوع دستکاری های غیرمجاز(صفر کردن شمارنده گام) توسط گره های مخرب به جهت جلب توجه گره مبدا می باشد.

۳- طراحی و تنظیم جدولی شامل لیست تمام گره های مشارکت کننده در کوتاه ترین مسیرها که دارای پارامترهایی از قبیل شناسه مسیرهای انتخابی و میزان مشارکت هر گره در فعالیت های شبکه می باشد.

جدول ۱- محاسبه میزان مشارکت

N	S۱	S۲	.....	Sn	TOTAL
N۱					
N۲					
.....					
Nn					

۴- در ادامه برای هر گره در صورت مشارکت آن در مسیرهای انتخابی عدد یک و در صورت عدم مشارکت عدد صفر را در هر یک از ستون های مسیرهای انتخابی درج نموده و در ستون آخر نیز مجموع تمام مشارکت ها را محاسبه خواهیم کرد. الگوریتم مورد استفاده جهت گرفتن خروجی های لازم از این جدول به صورت $CN_K = \sum_{i=1}^{n} Si$ تعریف شده است. جدول ۲ یک نمونه فرضی از نحوه عملکرد این الگوریتم در پارت اول را نشان می دهد.

جدول ۲- مثالی از محاسبه میزان مشارکت در پارت اول از فاز اول

N	S	S۱	S۲	S۳	S۴	S۵	S۶	S۷	S۸	S۹	S۱۰	$CN_K = \sum_{i=1}^{n} Si$
N۱		۱	۰	۱	۰	۱	۱	۰	۱	۰	۰	۵
N۲		۰	۱	۰	۰	۰	۱	۰	۰	۰	۰	۲
N۳		۱	۱	۰	۰	۱	۱	۱	۱	۱	۰	۷
N۴		۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱۰
N۵		۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۱
N۶		۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱۰
N۷		۱	۱	۰	۰	۰	۰	۱	۰	۰	۱	۴
N۸		۱	۱	۱	۱	۰	۱	۱	۱	۱	۱	۹
N۹		۰	۰	۱	۱	۰	۰	۰	۰	۱	۰	۳
N۱۰		۱	۱	۰	۱	۱	۱	۱	۰	۱	۱	۸

۵- از خروجی جدول ۲ گره هایی با میزان مشارکت مساوی و یا بالای ۵۰ درصد $\frac{1}{n} \leq CN_K$ انتخاب و به جدولی دیگر منتقل خواهند شد. این گره ها، کاندید اولیه نام دارند.

۶- در جدول ۳ (پارت دوم از فاز اول) پیشینه فعالیتی هر گره کاندید اولیه از روی جداول به روز رسانی شده مربوط به هر گره در شبکه مشخص خواهد شد. ستون اول این جدول شامل نام گره های کاندید اولیه (NN) ، ستون دوم نشان دهنده تعداد همکاری های هر گره با شبکه تا آن لحظه (آخرین به روز رسانی) بر اساس جدول پیشینه هر گره و ستون سوم بیان گر سه پارامتر مهم یعنی تعداد گره های دارای ارتباط با گره کاندید اولیه تا آن لحظه، درصد بیشترین همکاری گره کاندید با یک یا چند گره از شبکه و عنوان گره یا کره های همکار با بیشترین درصد همکاری خواهد بود. در ستون چهارم این جدول نیز لیست گره های کاندید نهایی حمله کرم چاله بر اساس استخراج همکاری های پر تکرار در شبکه استخراج خواهد شد.

جدول ۳- ادامه مثالی از محاسبه میزان مشارکت در پارت دوم از فاز اول

NN	مجوع تعداد مشارکت در فعالیت های شبکه	بیشترین میزان عبور بسته از گره بر حسب درصد			کاندید نهایی
		تعداد همکاران	درصد همکاری	مهمترین همکار	
NN۱	۶۵	۱۳	٪۵۲	N۲	*
NN۳	۴۹	۹	٪۴۵	N۷	
NN۴	۹۰	۱	٪۱۰۰	N۱۸	*
NN۶	۲۳۰	۱۲	٪۸۷	N۱۵	*
NN۸	۱۳۴	۱۸	٪۷۵	N۹	*
NN۱۰	۸۲	۱۴	٪۲۵	N۱۱	

۲.۲. فاز دوم

در این فاز IDS پیشنهادی ما تعدادی بسته تله با اطلاعات صحیح اما فاقد اعتبار زمانی و به نوعی نامعتبر جهت ارسال به مقاصدی از پیش تعیین شده را میان گره هایی که آمادگی خود را جهت انجام آن تراکنش اعلام کرده و جزء لیست انتخابی در فاز اول نیز هستند توزیع می کند و با تحلیل ورودی های نزدیک ترین همسایه های به گره های دریافت کننده بسته های تله و نامعتبر متوجه می شود که گره دریافت کننده شبکه را دور زده و بسته را به مقصد مد نظر خود ارسال کرده است و به این صورت شناسایی گره مخاصم اول و در پی آن گره مخاصم همکارش ممکن خواهد شد. بی شک به جهت عدم ایجاد سربار برای شبکه ، کم حجم بودن بسته های تله ارسال شده جزء مهمترین شروط منطقی جهت عملیاتی شدن ایده مذکور می باشد. بخش های اجرایی این فاز شامل موارد زیر می باشد

۱- سیستم پیشنهادی ما به بررسی عملکرد و سلامت سنجی گره های کاندید نهایی می پردازد. این کار با ارسال تعدادی بسته تله برای هرگره به اندازه تعداد مسیرهای بهینه ای که هر گره بر اساس جدول ۲ در فاز یک در آن ها مشارکت خواهد داشت صورت می پذیرد.

۲- در ادامه رفتار گره های کاندید نهایی در قبال تعداد بسته های تله دریافت کرده که همگی دارای مقصدهای متفاوت اما مشخصی بوده اند بررسی و گره ای که مجددا تمام همکاری های خود را با یک گره همکار مشخص صورت داده باشد، شناسایی و به همراه گره مخاصم همکارش در شبکه ایزوله خواهد شد. در این فاز همچنین مشخص می شود که همکاری های سایر گره های کاندید در هر دو فاز با تعداد محدودتری از همسایگان، کاملا اتفاقی و بر حسب شرایط شبکه صورت گرفته است اما این موضوع در مورد حمله کنندگان کرم چاله که تمام ورودی و خروجی هایشان دوسویه و انحصاری می باشد، صدق نخواهد کرد.

جدول ۴ نشان می دهد که کدام یک از گره های کاندید نهایی می تواند در قالب رفتاری از پیش برنامه ریزی شده و در جهت ایجاد اختلال و یا تخریب شبکه در زمینه ی ارسال و دریافت بسته ها همچنان آماری شبیه به اطلاعات ثبت شده در جدول پیشینه فعالیتی را از خود برجای گذاشته و در واقع از طریق استفاده از تونل مجازی از پیش ایجاد شده، باز هم بسته های تله را با دور زدن شبکه و به کمک روند ماموریتی خود به مقصد معین شده ارسال کرده اند. در جدول ۴ ENTERED به معنی تعداد بسته های تله ای سپرده شده به هر گره کاندید و به جهت انجام ماموریتی مشخص و EXIT معرف تعداد بسته هایی است که از گره کاندید به سمت سایر گره های شبکه (همسایه) خارج شده اند.

جدول۴ – ادامه مثالی از محاسبه میزان مشارکت در فاز دوم

NN	ENTERED	EXIT		گره های کرم چاله
		SEND TO	TOTAL	
NN۱	۵	N۲	۱	
		N۵	۱	
		N۸	۱	
		N۱۳	۱	
		N۱۹	۱	
NN۴	۱۰	N۱۸	۱۰	***
NN۶	۱۰	N۹	۲	
		N۱۰	۴	
		N۱۳	۱	
		N۱۷	۳	
NN۸	۹	N۶	۱	
		N۹	۲	
		N۱۴	۱	
		N۱۵	۳	
		N۱۹	۱	
		N۲۰	۱	

۳.۲. فاز سوم

در فاز سوم گره های مخاصم که ماهیت حمله کرم چاله را دارا بوده و در فاز دوم مورد شناسایی قرار گرفته اند، به عنوان حمله کنندگان شبکه در بستر حمله کرم چاله، به سایر گره های موجود و سالم در شبکه معرفی شده تا شبکه از وجود آنها ایزوله شود.

۳. پیاده سازی روش پیشنهادی

برای پیاده سازی ایده مذکور از یک شبکه موردی سیار با مشخصاتی از جمله ابعاد ۱۰۰۰ در ۱۰۰۰ متر ، ترافیک CBR ، ۲۰ گره سیار موجود ، کانال ارتباطی بیسیم و پروتکل مسیریابی AODV استفاده شده است. همچنین حداکثر اندازه بسته های ارسالی ۱۰۲۴ بایت بوده و از شبکه در زمان های مجزای ۱۰۰،۸۰،۶۰،۴۰،۲۰ ثانیه خروجی گرفته خواهد شد. لازم به یادآوری است که هدف از ارائه این روش بررسی عملکرد پارامترهای نرخ اتلاف بسته ها، توان عملیاتی، تاخیر انتها به انتها و نرخ تحویل بسته ها در بستر شبکه موردی متحرک دارای حمله کرم چاله می باشد. نرم افزار و نسخه مورد استفاده در این شبیه سازی NS2[1] می باشد.

۱.۳. شرح کامل پروتکل مسیریابی AODV[2]

پروتکل مسیریابی بردار فاصله بر مبنای تقاضا برای استفاده توسط گره‌های بیسیم در یک شبکه موردی طراحی شده است. این پروتکل در شبکه‌های موردی دارای سازگاری سریعی با شرایط پیوندهای پویا، سربار حافظه، استفاده ی محدود از پهنای باند شبکه و مشخص کردن مسیرهای تک پخشی می باشد. این پروتکل به منظور تضمین عدم وجود حلقه که در پروتکل بردار فاصله کلاسیک وجود داشت، شماره ترتیب مقصد را مورد استفاده قرار می‌دهد. پروتکل AODV قابلیت‌های پویا بودن، خود آغازی و مسیریابی چندگامی را برای گره‌های بیسیم که می‌خواهند در ایجاد یک شبکه موردی شرکت نمایند، فراهم می‌نماید (پیرکینس و همکاان،۲۰۰۴).

[1] Network Simulator
[2] Ad-Hoc On-Demand Distance Vector

۴. نتایج شبیه سازی

جهت به دست آوردن نتایجی با دقت بالا هر کدام از پارامترهای شبکه مورد نظر با حالت های زیر در NS شبیه سازی شده است:

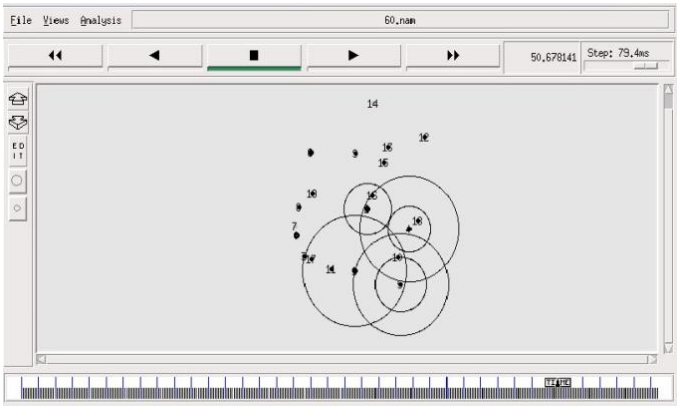
- شبکه بدون گره مخرب (AODV Standard)
- وجود گره مخرب کرم چاله در شبکه و عدم استفاده از روش پیشنهادی تشخیص نفوذ
- وجود گره مخرب کرم چاله در شبکه با استفاده روش پیشنهادی تشحیص نفوذ

جهت اطمینان از صحت نتایج برای هریک از حالت های بالا، شبکه را پنج بار به اجرا گذاشته و پس از تبت نتایج ، میانگین آنها در جداولی مجزا نشان داده شده است.

۱.۴. پارامترهای مورد ارزیابی

پارامترهای مورد نیاز جهت ارزیابی کارایی روش پیشنهادی به شرح زیر است.

- **نرخ اتلاف بسته :** برابر است با تعدادبسته های که به مقصد نرسیده اند.
- **توان عملیاتی :** معیاری برای سنجش توان عملیاتی در شبکه های موردی بیسیم می باشد که تعداد کارهای انجام شده را در واحد زمان را مشخص میکند.
- **تاخیر انتها به انتها:** میزان تاخیر انتها به انتها را در شبکه های موردی بیسیم را محاسبه میکند که برابر ست با زمان شروع ارسال بسته به مقصد منهای زمان رسیدن همان بسته به مقصد.
- **نرخ تحویل بسته:** متوسط نرخ تحویل بسته در شبکه های موردی بیسیم بوده که برابر است با نسبت تعداد بسته های رسیده تقسیم بر تعدادکل بسته های ارسالی.



شکل ۲- نمونه ای از یک لحظه فعالیت شبکه موردی با ایده پیشنهادی

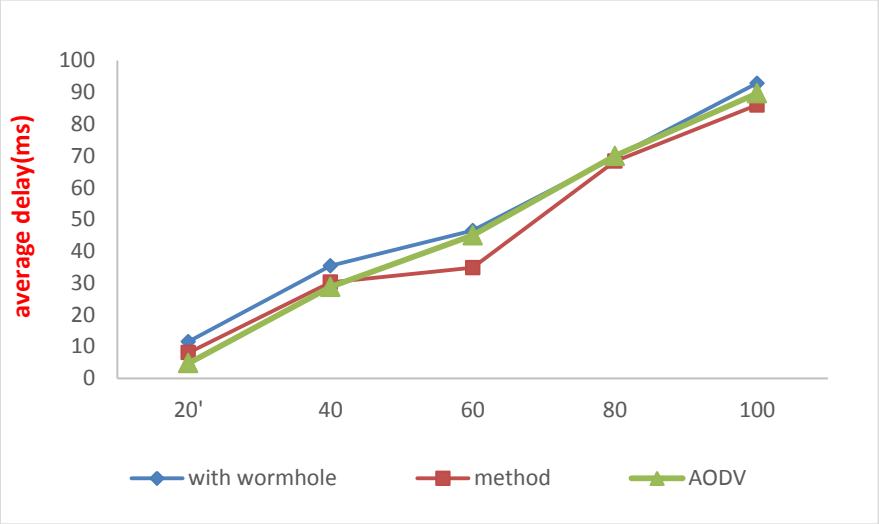
۱.۱.۴. تجزیه و تحلیل داده‌ها

در این بخش داده های بدست آمده را برای هریک از پارامتر های ذکر شده بصورت مجزا و برای تمام حالت های بیان شده مورد برسی و تجزیه و تحلیل قرار خواهیم داد و در چند پارامتر نیز خروجی های شبیه سازی مربوط به ایده پیشنهادی را با مقاله ای چاپ شده در همین زمینه و در مورد همین موضوع مقایسه خواهیم نمود.

- **میانگین تاخیر انتها به انتها**

جدول ۵- میانگین تاخیر انتها به انتها

Times	With Worm Hole	Method	AODV Standard
۲۰	۱۱/۵۸۵	۸/۰۸۶	۴/۷۷۱۹۴
۴۰	۳۵/۴۵	۳۰/۲۴۷۱	۲۸/۷۷۷
۶۰	۴۶/۴۹	۳۴/۸۳۴۶	۴۵/۰۱۹۸
۸۰	۶۹/۶۳۲	۶۸/۳۳۲	۶۹/۹۸۳۵
۱۰۰	۹۲/۸۱	۸۵/۹۵۶۵	۸۹/۶۵۳۳



شکل ۳ - میانگین عملکرد پارامتر تاخیر انتها به انتها در ۳ حالت شبیه سازی شبکه

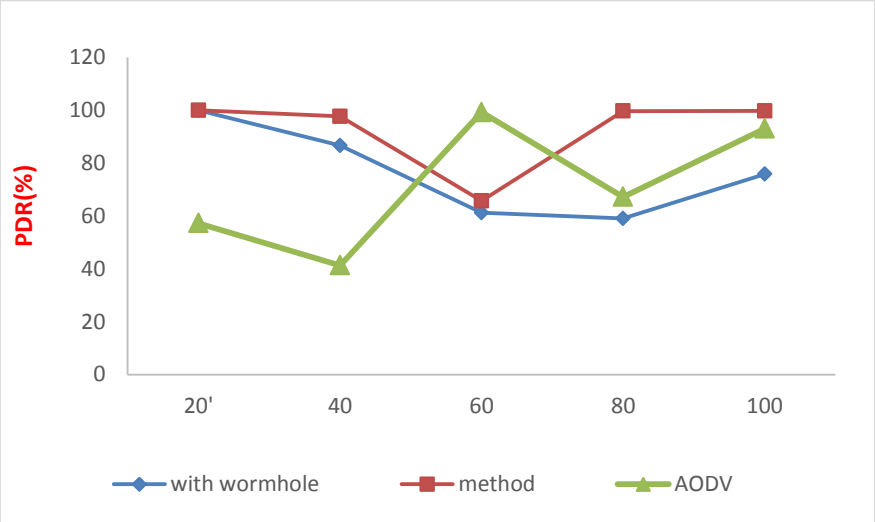
به طور کلی منظور از تاخیر، مدت زمانی است که طول می کشد تا بسته ای از مبدا به مقصد برسد و این زمان با تفریق زمان دریافت از زمان ارسال بسته به دست خواهد آمد. باید گفت که پارامتر تاخیر انتها به انتها برای تحلیل صحیح تعداد بسته هایی که توسط گره مبدا فرستاده شده و بطور موفق به مقصد رسیده اند مورد استفاده قرار گرفته که طبیعتا هرچه میزان این تاخیر کمتر باشد شبکه دارای عملکردی بهتر و کارایی بیشتری خواهد بود که مطلوب است استفاده از روش پیشنهادی جهت تشخیص گره های مخرب میزان تاخیر انتها به انتها را بیشتر از حد انتظار نکند.

همانطور که در نمودار ۳ مشاهده می شود پروتکل ارائه شده (method) نسبت به دو حالت دیگر در بعضی از زمان ها نرخ تحویل بسته بهتری دارد که می توان علت این امر را انتخاب مسیرهایی با تعداد گام و فاصله کمتر و همچنین تشخیص نفوذ گره های مخرب و ایزوله کردن آن ها دانست. ایده پیشنهادی در این پارامتر توانسته است در زمان های ۱۰۰-۸۰-۶۰ تاخیر انتها به انتهای شبکه را بهبود بخشیده و در زمان های ۴۰-۲۰ نیز عملکردی بهتر نسبت به شرایط وجود حمله کرم چاله در شبکه اما بدون استفاده از ایده پیشنهادی مذکور را از خود برجای بگذارد. بنابراین با توجه به متد پیشنهاد شده، طول مسیر در سه زمان نسبت به دو حالت دیگر کاهش یافته و بسته نیز نسبت به پروتکل دیگر زودتر به مقصد خواهد رسید که درنتیجه این اتفاق، تاخیر انتها به انتهای شبکه با کاهشی مثبت مواجه خواهد شد.

- **میانگین نرخ تحویل بسته ها**

جدول ۶ – میانگین نرخ تحویل بسته ها

Times	With Worm Hole	Method	AODV Standard
۲۰	۱۰۰	۱۰۰	۵۷/۲۸۱۶
۴۰	۸۶/۶۶۶	۹۷/۷	۴۱/۳۳۳
۶۰	۶۱/۲۷	۶۵/۷	۹۹/۲۶
۸۰	۵۹/۰۷	۹۹/۷۲	۶۷/۲۲۸۴
۱۰۰	۷۵/۸۴	۹۹/۷۸۹۳	۹۳/۰۴۳۵



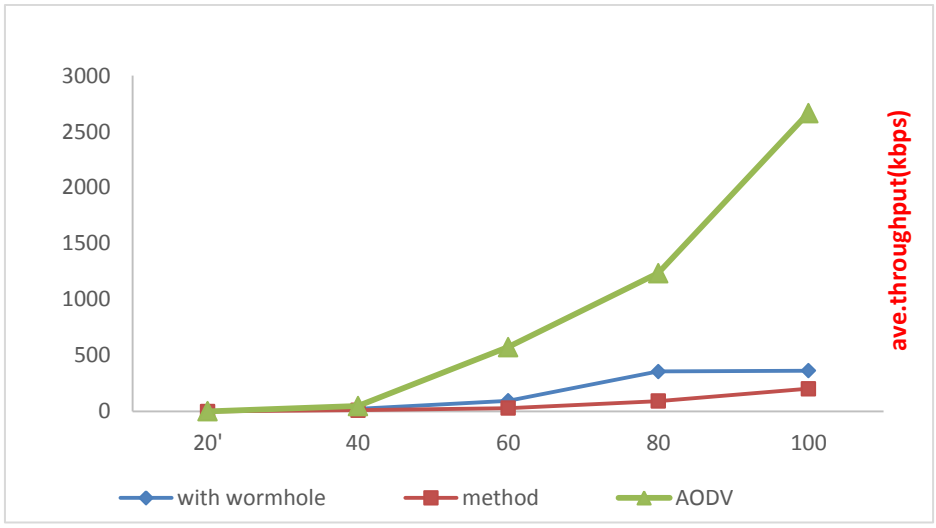
شکل ۴ – میانگین عملکرد پارامتر نرخ تحویل بسته ها در ۳ حالت شبیه سازی شبکه

نمودار ۴ نشان دهنده مقایسه سه پروتکل AODV استاندارد و روش پیشنهادی و شبکه تحت حمله می باشد. همانطور که در نمودار ۴ مشاهده می شود، پروتکل ارائه شده(method) نسبت به دوحالت دیگر نرخ تحویل بسته بهتری دارد و علت این امر انتخاب مسیرهای بهتر با تعداد گام کمتر و عدم وجود گره مخرب در طول مسیر و همچنین کل شبکه است. بدیهی است که هرچه نرخ تحویل بسته در شبکه بیشتر باشد، عملکرد شبکه قوی تر خواهد بود. بهترین مقادیر مطلوب حاصل از اجرای روش پیشنهادی در زمان های ۲۰,۴۰,۸۰,۱۰۰ ثانیه به ثبت رسیده است. در این زمان ها نرخ تحویل بسته افزایش یافته و در حالت بهتری قرار دارد که این نشان دهنده عملکرد بهتر روش پیشنهادی خواهد بود.

- **میانگین توان عملیاتی**

جدول ۷ – میانگین توان عملیاتی

Times	With Worm Hole	Method	AODV Standard
۲۰	۳/۰۰۴	۰/۰۸۳۳۵	۱/۶۷۷
۴۰	۲۳/۱۴۳۱	۱۱/۵۲۴۲	۴۸/۱۵۴
۶۰	۹۴/۹۷۸	۳۰/۵۵۹۶	۵۷۴/۹۸
۸۰	۳۵۶/۷۵	۹۲/۳	۱۲۳۵/۹
۱۰۰	۳۶۳/۸۸۱	۲۰۲/۶۸۵	۲۶۶۵/۰۹



شکل ۵ - میانگین عملکرد پارامتر توان عملیاتی در ۳ حالت شبیه سازی شبکه

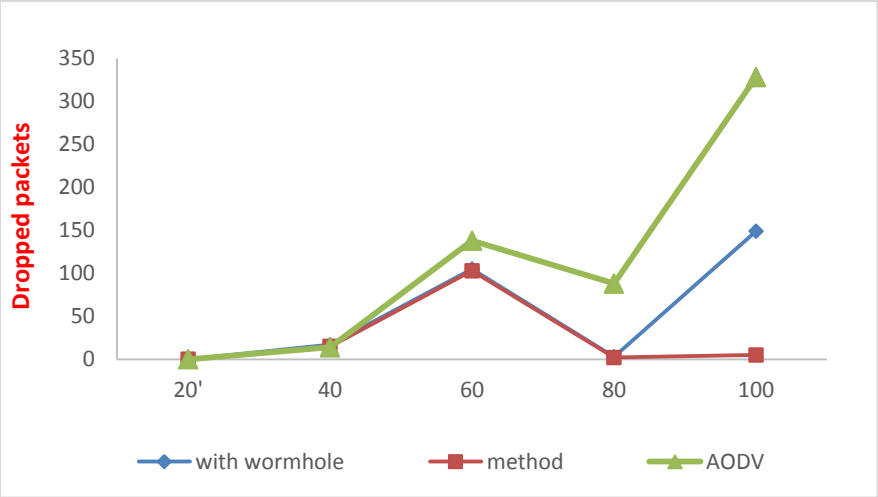
توان عملیاتی در یک شبکه از مقایسه تعداد تمام بسته های رسیده به مقصد، نسبت به زمان شبیه سازی شده شبکه به دست خواهد آمد. این پارامتر به عبارتی نشان دهنده ی توازن بار در شبکه است. توان عملیاتی با تقسیم اندازه بسته در هر زمان، در واحد مگابیت (megabit) بر ثانیه، کیلوبیت (kilobit) بر ثانیه و یا بیت بر ثانیه استخراج می شود.

نمودار ۵ نشان دهنده مقایسه توان عملیاتی سه حالت AODV استاندارد و شبکه تحت حمله و شبکه تحت روش پیشنهادی می باشد. همانطور که در نمودار ۵ مشاهده می شود پروتکل ارائه شده (method) نسبت به دو پروتکل دیگر دارای توان عملیاتی بهتری نبوده و در واقع روش پیشنهادی به سبب کشف و حذف گره های مخاصم حمله کرم چاله و همچین ایزوله کردن شبکه و نیز کاهش محسوس تعداد گره های موجود در شبکه نمی تواند در بهبود پارامتر توان عملیاتی شبکه موردی موثر واقع شود که این اتفاق با توجه به ماهیت حملات کرم چاله کاملا طبیعی خواهد بود. اما بدیهی است که پس از ایزوله شدن و کاهش تعداد گره های مسیریاب شبکه به مجموعه ای از سالم ترین گره ها ، در مقابل کاهش پارامتر توان عملیاتی شبکه ، پارامتر نرخ تحویل بسته در شبکه با افزایشی قابل تامل مواجه خواهد شد که در نتایج به دست آمده از ایده پیشنهادی مذکور این ادعا به اثبات رسیده است.

- **میانگین نرخ اتلاف بسته ها**

جدول ۸- میانگین نرخ اتلاف بسته ها

Times	With Worm Hole	Method	AODV Standard
۲۰	۰	۰	۰
۴۰	۱۷	۱۵	۱۴
۶۰	۱۰۵	۱۰۳	۱۳۸
۸۰	۳	۲	۸۸
۱۰۰	۱۴۹	۵	۳۲۸



شکل ۶ - میانگین عملکرد پارامتر نرخ اتلاف بسته ها در ۳ حالت شبیه سازی شبکه

همانطور که در نمودار ۶ مشاهده می شود پروتکل ارائه شده (method) نسبت به دو حالت دیگر توان نرخ اتلاف بسته کمتری دارد و علت این امر استفاده از روش پیشنهادی در جهت تشخیص گره مخرب است. در واقع از آنجا که هر اندازه میزان اتلاف بسته ها کمتر باشد ، عملکرد شبکه قابل قبول تر خواهد بود، در نمودار ۶ می توان مشاهده کرد که شبکه در حالت Aodv Standard (بدون حمله) نسبت به دیگر حالات دارای کمترین میزان اتلاف بسته ها خواهد بود و از این رو روش پیشنهادی هرچقدر به این حالت نزدیکتر باشد، کارایی آن بارز تر خواهد بود. به استناد نمودار ۶ ، میزان اتلاف بسته ها در شرایط وجود حمله کرم چاله در شبکه نسبت به حالت عدم استفاده از این روش، در زمان ۲۰ ثانیه برابر و در زمان های ۴۰-۶۰-۸۰-۱۰۰ ثانیه کاهش یافته است. از این رو با توجه به توضیحات فوق می توان نتیجه گرفت که روش پیشنهادی در بیشتر زمان ها کارآمد بوده و نرخ اتلاف بسته ها را نسبت به حالتی که از این روش استفاده نشده است کاهش داده و در تشخیص گره های مخرب موثر بوده است.

۵. نتیجه‌گیری

ارائه روشی نو و کارا جهت کشف حمله کرم چاله، اصلی ترین هدف این حقیق بوده که اکنون زمان آن رسیده تا به بررسی این امر بپردازیم که چقدر این هدف تحقق یافته و روش پیشنهادی چه میزان کارا و موثر واقع شده است. قطعا صرف نظر از اینکه روش پیشنهادی قادر به کشف حمله کرم چاله شده یا نه، جهت ارزیابی کارایی آن کافی نبوده و قابل قبول نیست زیرا همانگونه که پیش تر شرح داده شد، محدودیت منابع، سرعت در برپایی و کم هزینه بودن شبکه های موردی متحرک علت استفاده از شبکه ها را توجیح می کند، پس اگر الگوریتم پیشنهادی ما در راستای تقویت محاسن و پوشش معایب این شبکه ها گام بردارد، مطلوب بوده و مورد پذیرش قرار خواهد گرفت. در بخش قبل به معرفی برخی از پارامترهای ارزیابی شبکه های موردی پرداخته و همچنین به کمک جداولی مشخص، نتایج حاصل از اجرای شبیه سازی یک شبکه موردی در حالت های متفاوتی شرح و توضیح داده شد. سپس به کمک نمودارهایی این نتایج مورد ارزیابی و تفسیر قرار گرفته و عملکرد ۴ پارامتر اصلی شبکه در زمینه ایده پیشنهادی و در زمان های اجرایی مختلفی نشان داده شد که در ادامه به نتیجه گیری در همین باره خواهیم پرداخت.

در این پژوهش پارامتر نرخ اتلاف بسته ها با استفاده از ایده پیشنهادی و در حالتی که یک حمله به شبکه وارد شده باشد، در اکثر زمان ها با کاهش مواجه شده است و این موضوع کارآمد بودن ایده پیشنهادی در زمینه بهبود این پارامتر از شبکه را اثبات می کند. در مورد عملکرد این پارامتر بر مبنای ایده پیشنهادی باید گفت که نرخ اتلاف بسته ها در زمان اجرای ۲۰ ثانیه با

شرایط وجود حمله کرم چاله در شبکه برابر و در زمان های ۱۰۰-۸۰-۶۰-۲۰ ثانیه با کاهشی منطقی و مورد انتظار مواجه شده است. دیده می شود که پارامتر توان عملیاتی شبکه شبیه سازی شده در هیچکدام یک از زمان های اجرایی نسبت به حالت استاندارد شبکه و یا حالت وجود حمله کرم چاله در شبکه با افزایش مواجه نشده و گاهاً کاهش نیز یافته است که این نتیجه با توجه به هدف ایزوله کردن شبکه از وجود گره های شناسایی شده مخاصم کرم چاله در بخش فرضیات پژوهش، کاملا طبیعی و قابل پیش بینی بود چراکه قطعاً اگر بر اساس فرضیات ارائه شده تعدادی از گره های شبکه، حمله کنندگان کرم چاله بوده و ایده پیشنهادی با روند فعالیتی خود آنها را شناسایی و از شبکه حذف کند، شبکه با تعداد محدود تری از گره ها که البته دارای سلامت کاری بیشتری هستند مواجه شده که همین موضوع کاهش تعداد گره های فعال در شبکه نیز توان عملیاتی شبکه را کاهش خواهد داد. با توجه با نمودارهای استخراج شده می توان ادعا کرد که پس از ایزوله شدن شبکه از وجود گره های مخاصم کرم چاله، پارامتر تاخیر انتها به انتها در زمینه ارسال و دریافت بسته ها در شبکه شبیه سازی شده بر مبنای ایده پیشنهادی، در زمان های ۱۰۰-۸۰-۶۰ ثانیه با بهینگی مواجه شده و در زمان های ۴۰-۲۰ ثانیه نیز عملکردی بهتر نسبت به شرایط وجود حمله کرم چاله در شبکه موردی بدون استفاده از ایده پیشنهادی را از خود نشان می دهد. همچنین می توان اثبات کرد که به دلیل سلامت سنجی گره ها در مراحل قبلی، قطعاً پارامتر نرخ تحویل بسته ها در شبکه شبیه سازی شده دارای افزایشی معقول و قابل پذیرش می باشد چراکه بی شک با ایزوله کردن شبکه از وجود گره های مخاصم شناسایی شده حمله کرم چاله که خود به خود کاهش طبیعی توان عملیاتی شبکه را در پی خواهد داشت، شبکه با سلامت و امنیتی مضاعف مواجه شده که همین اتفاق نرخ تحویل بسته ها در زمان های ۱۰۰-۸۰-۴۰-۲۰ ثانیه را با افزایشی چشم گیر مواجه کرده است. در حقیقت و با توجه به توضیحات ارائه شده، می توان نتیجه گرفت که روش پیشنهادی ما می تواند به عنوان یک روش خوب و موثر جهت کشف و برخورد با گره های همکار حمله کننده کرم چاله در شبکه موردی، مورد استفاده و بهره برداری قرار گیرد. اگرچه نمی توان به قطعیت گفت که روش پیشنهادی این پژوهش نسبت به تمام روش های ارائه شده در این زمینه بهتر خواهد بود اما می توان ادعا کرد که خروجی عملکرد شبکه شبیه سازی شده با استفاده از این روش، نه بهبود قعی اما یک بهینگی نسبی در رابطه با شبکه های موردی متحرک را نشان داده و اثبات می کند. بی شک مقایسه نتایج حاصل از عملکرد این ایده پیشنهادی با تمام ایده های ارائه شده در این زمینه نیازمند یک تحقیق گسترده تر بوده که خود می تواند انگیزه و زمینه مناسبی جهت تحقیق و ادامه مبحث مورد پژوهش باشد.

۶. ارائه پیشنهادات

- هدف و کاربرد این تحقیق ارائه روشی نو جهت شناسایی گره های مخرب کرم چاله است که می توان این ایده را با ترکیب با روش های دیگر پیشنهاد شده توسعه بخشیده و جهت شناسایی دیگر حملات مربوط به شبکه های موردی متحرک از آن استفاده کرد.
- تحقیق در رابطه با ایده هایی ارائه شده در چهارچوب همین نوع از حمله در شبکه های موردی متحرک و مقایسه توان خروجی پارامترهای اصلی شبکه در این پژوهش با نتایج سایر پژوهش های مربوطه می تواند انگیزه و ایده مناسبی جهت انجام یک پژوهش تازه در همین زمینه را به دنبال داشته باشد.

۷. مراجع

1. Nivedha.s, SankaraNarayanan.s; “Detection and Prevention of Wormhole Attack in MANET using New Fresh Algorithm”; nternational Journal of Advanced Research in Computer Engineering & Technology; ISSN:2278 –1323. ;2015.

2. Neeraj Arya;Upendra singh;Sushma singh ;"Detecting and Avoiding of Worm Hole Attack and CollaborativeBlackhole attack on MANET using Trusted AODV Routing Algorithm"; IEEE International Conference on Computer, Communication and Control;2015.

3. Arvind Dhaka, Amita Nandal, Raghuveer S. Dhaka;"Gray and Black Hole Attack Identification usingControl Packets in MANETs"; Eleventh International Multi-Conference on Information Processing; Procedia Computer Science 54 ; 83 – 91;2015.

4. Imran.M, Aslam Khan.F, Jamal.T, Hanif Durad.M ; "Analysis of Detection Features for Wormhole Attacks in MANETs"; International Workshop on Cyber Security and Digital Investigatio; Procedia Computer Science 56 ; 384 – 390;2015.

5. Fotohi.R , Jamali.Sh; "A Comprehensive Study on Defence Against Wormhole Attack Methods in Mobile Ad hoc Networks "; International journal of Computer Science & Network Solutions ;Volume 2.No5;ISSN 2345-3397;2014.

6. Mehto, A.; Gupta, H.;"A dynamic hybrid approach for wormhole detection and prevention ",Computing, Communications and Networking Technologies (ICCCNT), 10.1109/ICCCNT. 6726564;2013.

7. Nisha S.Raote;"Defending Wormhole Attack in Wireless Ad-hoc Network"; International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.3;Nagpur, India;2011.

8. Hu.Y.C, Perrig.A , Johnson,D.B;"Packet leashes: a defense against wormhole attacks in wireless networks"; in In Proce ; of IEEE INFOCOM;2003.

9. Hu.L , Evans.D;"Using directional antennas to prevent wormhole attacks"; in Network and Distributed System Security Symposium (NDSS); San Diego;2004.

10. Wang.X , Wong.J;"An end-to-end detection of wormhole attack in wireless ad-hoc networks"; iIn Proc. of International. Conference on Computer Software and Applica- tions;2007.

11. Gupta, S., Kar, S., Dharmaraja, S; "WHOP: Wormhole attack detection protocol using hound packet" ; International Conference on Innovations in Information Technology (IIT), pp.226-231, 25-27;2011.

12. Khan, Z.A., Islam, M.H;"Wormhole attack: A new detection technique". International Conference on Emerging Technologies (ICET), pp.1-6, 8-9; 2012.

13. Shukla, R.K.; Upadhyay, V.K.; Dubey, R.;"Detection and prevention of worm holes in mobile ad-hoc networks using Hybrid Methodology"; IT in Business, Industry and Government (CSIBIG), 10.1109/CSIBIG .7056993;2014.

14. Neeraj Arya;Upendra singh;Sushma singh;"Detecting and Avoiding of Worm Hole Attack and CollaborativeBlackhole attack on MANET using Trusted AODV Routing Algorithm"; IEEE International Conference on Computer, Communication and Control; 2015.