به نام خداوند بخشاینده مهربان

کشف و حذف حمله سیاهچاله جمعی در شبکه های سیار ادهاک

ارائه کننده:
مهدی مدادیان

تعریف شبکه ادهاک

63/3

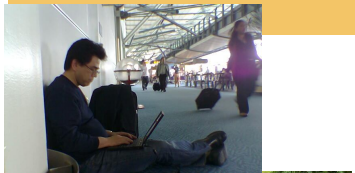
- شبکه های ویژه سیار مجموعه ای از گره های بی سیم هستند که

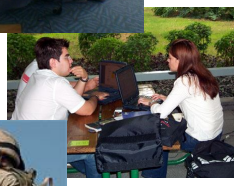
  - می توانند به صورت پویا در هر مکان و در هر زمان بدون استفاده از هر زیرساخت شبکه ای ایجاد شوند
  - گره ها در آن واحد هم به عنوان مسیریاب و هم به عنوان گره عمل می کنند
  - در موارد اضطراری که امکان تشکیل شبکه ای با ساختار ثابت وجود ندارد مثل موارد نظامی، وقوع سیل و...
  - ارتباط میان گره ها از طریق امواج رادیویی صورت می گیرد، در صورتی که یک گره در برد رادیویی گره دیگر باشد همسایه آن گره محسوب می شود
  - در صورت نیاز به ارتباط میان دو گره که در برد رادیویی یکدیگر نیستند می توان از کمک گره های دیگر در این مورد استفاده کرد بنابراین

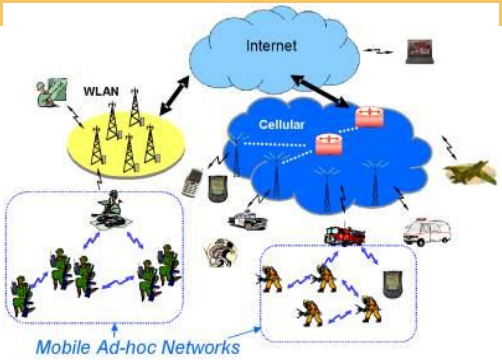
ارتباط میان گره ها در این شبکه به نوعی بر مبنای اعتماد و مشارکت میان گره ها صورت می گیرد

کاربردهایی از شبکه ادهاک

63/4





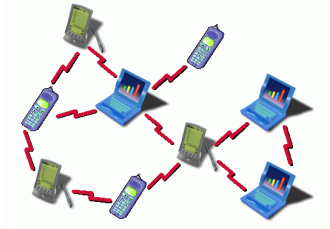


63/5 مشخصات شبکه های ادهاک

- ترمینال های خودمختار
- توزیع شدگی
- مسیریابی چندگامه
  - در صورتی که گره مبدأ و گره مقصد در محدوده رادیویی یکدیگر نباشند در این صورت یک مسیریابی چندگامه مورد نیاز است.
- توپولوژی پویای شبکه
- پهنای باند نوسان دار
- ترمینال های ضعیف

63/6 مسیریابی در شبکه های ادهاک

- به علت عدم وجود ساختار ثابت، مسیریابی در شبکه های ادهاک بر عهده خود گره هاست.
- هیچ دستگاه کمک شبکه ای مانند سوییچ، مسیریاب و یا hub برای مسیریابی وجود ندارد.



چگونه خود گره ها می توانند عمل مسیریابی در شبکه را انجام دهند؟

I. Flooding
II. AODV
III. DSR

63/7 الگوریتم Flooding برای انتقال اطلاعات

- ساده ترین راه حل برای حل مشکل مسیریابی در شبکه های موردی، انتقال اطلاعات از طریق flooding است. در این روش :
  - فرستنده اطلاعات، بسته ها را برای تمامی گره های همسایه خود ارسال می کند.
  - هر گره که یک بسته اطلاعاتی را دریافت می کند نیز این اطلاعات را برای همسایه های خود می فرستد.
  - برای جلوگیری از ارسال یک بسته توسط یک گره برای بیش از یک بار، از یک شماره توالی برای هر بسته استفاده می شود.
  - با این روش داده به طور حتم به مقصد خواهد رسید ولی بعد از رسیدن اطلاعات به مقصد، عملیات flooding همچنان ادامه پیدا می کند تا بسته، به تمامی گره های موجود در شبکه برسد.

63/8 مزایا و معایب الگوریتم Flooding

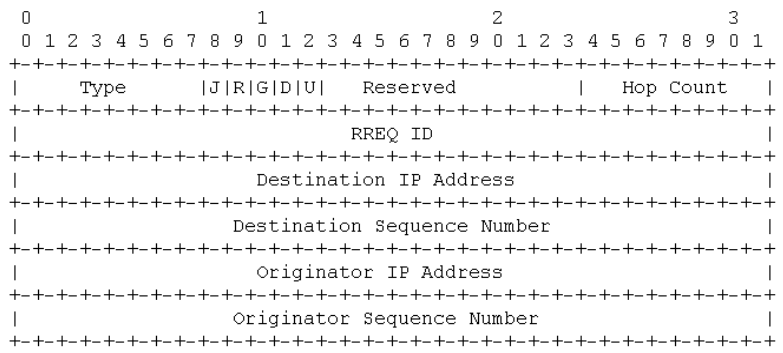
- **مزیت اصلی** این روش در درجه اول سهولت پیاده سازی آن و در درجه دوم اطمینان از دستیابی بسته به مقصد است.
- ولی **اشکال عمده** در این طرح این است که بسته های داده غالبا از حجم بالایی برخودار هستند و داده ها ممکن است مسافتی را بدون آن که لازم باشد طی کنند.
- همین افزایش شدید بار شبکه باعث می شود تا از روش flooding برای انتقال اطلاعات استفاده نشود. ولی این روش در جابجایی سیگنالهای کنترلی به دلیل حجم کوچک این سیگنالها، استفاده فراوانی دارد.
  - بسته های کنترلی بسته هایی هستند که برای بدست آوردن مسیر از آنها استفاده می شود.

63/9 پروتکل مسیریابی AODV

- الگوریتمی است که بنا به تقاضا کار می کند، به این معنی که مسیر بین گره ها را تنها در صورتی که توسط گره منبع درخواست شده باشد، می سازد.
- سربار حافظه کمی دارد.
- سازگاری سریع با پویایی شبکه دارد.
- برای جلوگیری از وقوع حلقه و تضمین تازگی مسیر از شماره دنباله استفاده می کند.
- این الگوریتم مسیرها را تنها تا زمانی که توسط منبع مورد نیاز است حفظ می کند.
- برای مقیاس های بزرگ شبکه که از تعداد زیادی گره موبایل تشکیل شده است، هم پاسخگوست.
- AODV با استفاده از یک چرخه پرس‌وجوی درخواست مسیر و پاسخ مسیر، مسیرها را می‌سازد.

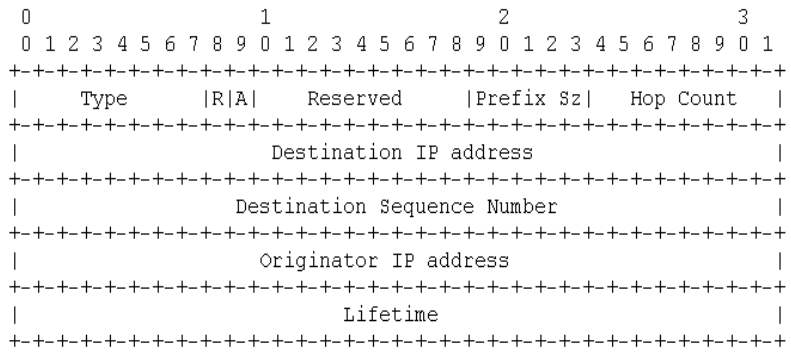
63/10 پیغام RREQ یا درخواست مسیر

- پیغام RREQ پیغام درخواست مسیر است که برای ایجاد یک مسیر از منبع به مقصد تولید می‌شود که با Flood این پیغام در شبکه، کشف مسیر انجام می شود.



63/11 پیغام RREP یا پاسخ مسیر

- پس از اتمام مرحله ارسال کردن بسته درخواست مسیر، پیغام RREP از گره مقصد در جهت معکوس برای گره مبدأ ارسال می‌شود.



63/12 روش کار AODV

- وقتی که گره مبدأ درخواست مسیری به مقصدی را می‌کند، گره ایی که در حال حاضر مسیری به مقصد ندارد، بسته درخواست مسیر را به صورت broadcast به سراسر شبکه ارسال می‌کند. گره هایی که این بسته را دریافت می‌کنند، اطلاعاتشان را بنا به اطلاعات گره مبدأ، بروز کرده و یک مدخل مسیر معکوس را برای مبدأ در جداول مسیر خود ایجاد می‌کنند.

- گره دریافت کننده RREQ، در صورتیکه خودش گره مقصد باشد و یا مسیری به مقصد با شماره ترتیب بزرگتر یا مساوی شماره ترتیب RREQ داشته باشد، پاسخ RREQ را ارسال خواهد کرد. در *غیر اینصورت* :

- گره دریافت کننده مجدداً RREQ را بصورت broadcast ارسال می کند.

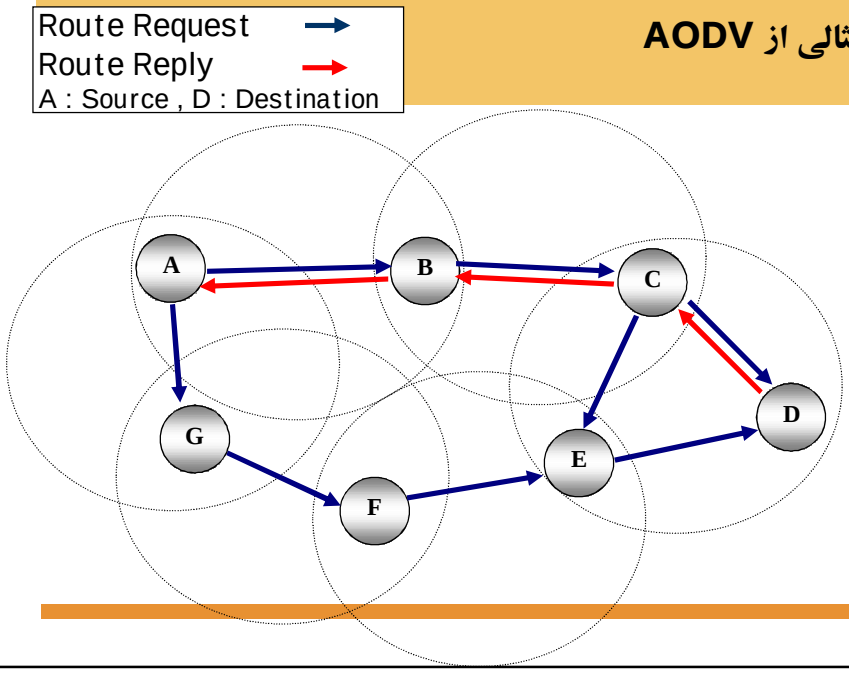
63/13 روش کار AODV - ادامه

- اگر بعداً منبع، RREP ای که شامل یک شماره ترتیب بزرگتر است یا شماره ترتیب یکسان با تعداد hop count کوچکتر را دریافت کند، اطلاعات مسیریابی مربوط به مقصد را بروز کرده و مسیر بهتر را مورد استفاده قرار می‌دهد.

- الگوریتم AODV به گره های سیار اجازه می‌دهد که مسیریابی برای مقصدهای جدید را به سرعت انجام دهند و نیازی ندارد که گره ها، مسیرهای به مقصد را که در ارتباط فعال نیستند، نگه دارند. وقتی که لینکها قطع می‌شوند، AODV به مجموعه گره هایی که مسیر را تشکیل می‌دهند، خبر ازدست رفتن لینک را می‌دهد و آنها را از شکستن لینک آگاه می‌کند.

- اگر قطع شدن یک اتصال درحالیکه مسیر فعال است اتفاق بیافتد، یک پیغام خطای مسیر RERR ارسال می‌شود.

63/14 مثالی از AODV



63/15 الگوریتم DSR

- درالگوریتم مسیریابی DSR، گره مبدا یک بسته به نام RREQ تولید کرده و در آن، گره مبدا و مقصد را مشخص می کند و این بسته را به وسیله الگوریتم flooding ارسال می کند.
- در الگوریتم DSR هر گره دارای Route Cache است که در آن، اطلاعات مسیرهایی که آن گره در طول زمان شنیده یا یاد گرفته، نگهداری می شود.

63/16 الگوریتم DSR- ادامه

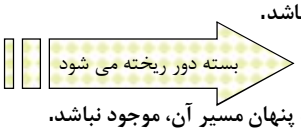
- هر گره با دریافت یک بسته RREQ، در صورتی که :

A. گره مزبور، مقصد بسته **ROUTE REQUEST** نباشد.

B. گره مزبور در مسیر مبدأ، لیست نشده باشد.

C. بسته تکراری نباشد.

D. هیچ اطلاعات مسیری به سوی مقصد، در حافظه پنهان مسیر آن، موجود نباشد.



آنگاه نام خود را به لیست بسته اضافه کرده و آن را Broadcast می کند.

- وقتی بسته به مقصد می رسد، یک بسته حاوی اطلاعات گره های مسیر و ترتیب آنها در دست گره مقصد وجود دارد. گره مقصد یک بسته RREP ایجاد کرده و آن را از روی لیست موجود در سرآیند بسته RREQ برمی گرداند.

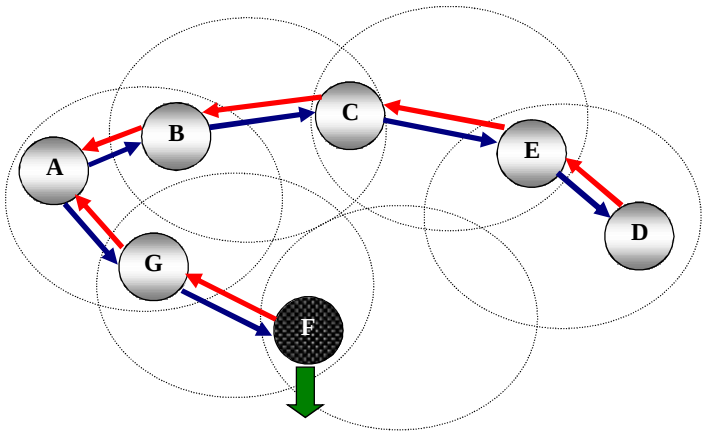
63/17 الگوریتم DSR- ادامه

- گره های میانی از روی لیست موجود می دانند که بسته را می بایست برای چه کسی ارسال نمایند. بنابراین بسته مسیر را به صورت برعکس طی می کند تا به گره مبدا برسد.
- بعد از کشف مسیر، فرستنده داده می تواند مسیر مقصد را در سرآیند داده ارسالی قرار دهد تا گره های میانی از طریق این مسیر، بدانند که باید بسته را به چه کسی ارسال نمایند.
- هنگامی که یک گره نتواند بسته داده را به گره بعدی ارسال نماید، بسته ای با نام RERR تولید نموده و آن را بر روی مسیر، بازمی گرداند. بدین ترتیب گره های دریافت کننده RERR متوجه قطع ارتباط بین آن دو گره می شوند.

63/18 حمله سیاهچاله و انواع آن

Route Request
Route Reply
Data
A : Source
D : Destination
F : Black Hole

- سیاه چاله



63/19 پیشینه تحقیق

- یک سیاه چاله، گره ای بدرفتار است که به هر درخواستی مسیر بدون داشتن مسیر فعالی به مقصد مشخص، به دروغ پاسخ می دهد وهمه بسته های دریافتی را دور می ریزد.

- گره های سیاه چاله ممکن است مانند یک گروه کار کنند به این معنی که بیشتر از یک گره سیاه چاله به صورت جمعی کار کنند تا گره های دیگر را، اشتباه راهنمایی کنند. این نوع از حمله، حمله سیاه چاله جمعی نامیده می شود.

63/20 پیشینه تحقیق-ادامه

- در [1] راه حلی برای سیاه چاله تکی پیشنهاد شده است. در این روش:
  - **اطلاعات گام بعدی به مقصد، باید وقتی که هر گره میانی به RREQ پاسخ می دهد، ضمیمه بسته RREP شود، سپس گره مبداء یک درخواست مجدد (FREQ) به گام بعدی گره پاسخگو می فرستد و درباره گره پاسخگو و مسیر به مقصد می پرسد.**
  - **با استفاده از این روش می توان قابلیت اعتماد گره پاسخگو را تنها اگر گام بعدی قابل اعتماد باشد، شناسایی کرد.**
  - **این راه حل نمی تواند از حمله سیاه چاله جمعی در MANETها پیشگیری کند.**

63/21 پیشینه تحقیق-ادامه

- در [2] نیز راه حلی برای کشف سیاه چاله تکی ارائه شده است. در این روش:
  - درخواست تایید مسیر یا **CREQ** را به گره **hop** بعدی در جهت مقصد می فرستد.
  - بعد از آن که، گره **hop** بعدی، **CREQ** را دریافت کرد، جدول مسیر خودش را برای پیدا کردن یک مسیر به مقصد جستجو می کند.
  - اگر مسیری داشته باشد آنگاه پاسخ تایید مسیر یا **CREP** را به همراه اطلاعات مسیر به گره مبداء می فرستد.
  - گره مبداء با مقایسه اطلاعات **CREP** تشخیص می دهد مسیر موجود در **RREP** معتبر است یا خیر.
  - چون عملیاتی به پروتکل مسیریابی اضافه شده در نتیجه سربار این روش بالاست.

63/22 پیشینه تحقیق-ادامه

- در [3]:
  - گره مبداء با پیدا کردن بیشتر از یک مسیر به مقصد، اعتبار گره ای که **RREP** را شروع کرده، تایید می کند.
  - گره مبداء صبر می کند تا بسته **RREP** را از بیش از دو گره دریافت کند. در شبکه های ادهاک، در مسیرهای تکراری در بیشتر اوقات تعدای گره و **hop** مشترک وجود دارد.
  - وقتی گره مبداء **RREP**ها را دریافت کرد، در صورتی که در مسیرها به مقصد، **hop**های مشترک وجود داشته باشد، گره مبداء می تواند مسیر ایمن به مقصد را تشخیص دهد.
  - این روش باعث تاخیر مسیریابی می شود چون گره باید منتظر بماند تا **RREP** را از بیش از دو گره دریافت کند.

63/23 پیشینه تحقیق-ادامه

- در [4] یک روش ارائه شده است که حمله سیاه چاله جمعی را شناسایی می کند:
  - **این روش با استفاده از جدول اطلاعات مسیریابی داده (DRI)، پیغام FREQ و پاسخ مجدد (FREP) پیاده سازی می شود.**
  - **هر گره یک جدول اطلاعات مسیریابی را نگهداری می کند. DRI پیگیری می کند که آیا گره با همسایگانش تبادل داده داشته است یا خیر. در این جدول مدخلی برای هر همسایه نگهداری می شود.**
  - **DRI نشان می دهد که آیا گره از طریق این همسایه داده فرستاده یا خیر و همچنین آیا گره از این همسایه داده دریافت کرده است یا خیر.**

63/24 پیشینه تحقیق-ادامه

- در [5] یک راه حل دیگر که از وقوع حمله سیاه چاله جمعی جلوگیری می کند، ارائه شده است.
- در این روش برای مقابله با حملات سیاه چاله از جدول صحت استفاده می شود که در آن هر گره شرکت کننده یک درجه صحت دارد که به عنوان اندازه اطمینان آن گره محسوب می شود.
- اگر درجه صحت یک گره صفر شود به این معنی است که این گره، یک گره متخاصم است که اصطلاحا به آن سیاه چاله گفته می شود که باید دور ریخته شود.

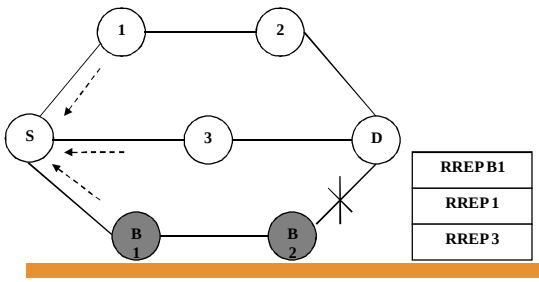
63/25 پیشینه تحقیق-ادامه

- گره مبداء RREQ را به همسایگانش می فرستد. پس از آن مبداء به اندازه TIMER منتظر می ماند تا پاسخ های RREP جمع آوری شوند.
- در هر کدام از RREPهای دریافتی، درجه صحت گره پاسخ دهنده مشخص است، برای هر کدام از آن ها درجه صحت گام بعدی آن ها، بررسی می شود.
- اگر دو یا بیشتر از دو مسیر که درجه صحت یکسانی دارند، وجود داشت آنگاه آن مسیری انتخاب می شود که تعداد گام کمتری داشته باشد در غیر اینصورت مسیری که درجه صحت بیشتری دارد انتخاب می شود.

63/26 پیشینه تحقیق-ادامه

- با دریافت بسته های اطلاعاتی، گره مقصد یک تصدیق دریافت (ack) به مبداء می فرستد که بوسیله آن درجه صحت گره میانی افزایش می یابد، اگر ack دریافت نشد آنگاه درجه صحت گره میانی کاهش می یابد.
- اصول کاری روش پیشنهاد شده در [5] به صورت زیر است:

1) جمع آوری پاسخ ها :
   - ✓ آدرس مبداء
   - ✓ آدرس مقصد
   - ✓ تعداد گام
   - ✓ گام بعدی
   - ✓ طول عمر
   - ✓ شماره دنباله مقصد



63/27 پیشینه تحقیق-ادامه

2) انتخاب یک پاسخ از بین پاسخ های رسیده :

- درجه های صحت گره پاسخ دهنده و گام بعدی اش جستجو می شود. اگر میانگین درجه های آن ها بیشتر از حد آستانه باشد آنگاه گره قابل اعتماد در نظر گرفته می شود.
- در صورت رسیدن چندین پاسخ، آن پاسخی انتخاب می شود که بیشترین درجه صحت را دارد.
- در صورتیکه درجه صحت دو گره یکسان باشد، آن گره ای انتخاب می شود که تعداد گام کمتری دارد.

3) به روز رسانی جدول صحت :

4) حذف سیاه چاله :

63/28 روش پیشنهادی

- در 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:

1) 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

2) ارسال بسته درخواست نظرات همسایه ها در مورد یک گره همسایه که بسته RREP را ارسال کرده است.

3) دریافت اطلاعات ثبت شده در گره های همسایه در مورد گره فرستنده بسته RREP

63/29 روش پیشنهادی-ادامه

4) بررسی اطلاعات دریافتی و اعلام نظر در مورد خرابکار بودن گره.
5) ارسال یک بسته خطر برای قرنطینه کردن گره خرابکار.
6) حذف گره های داخل قرنطینه در فرآیند مسیریابی.

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

1) 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.

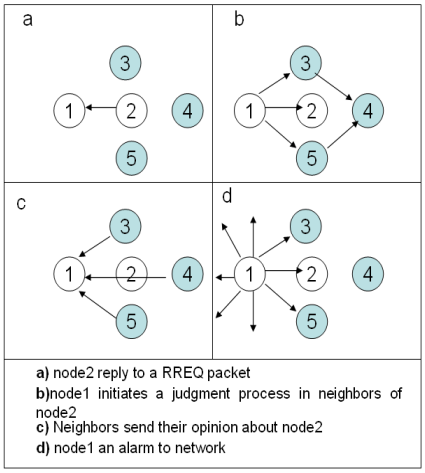
2) هر گره دارای لیستی از گره هایی است که در قرنطینه می باشند و باید این گره ها را از فرآیند مسیریابی حذف کرد.

63/30 روش پیشنهادی-ادامه

- 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 گره‌های 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.

63/31 تشخیص خرابکار بودن یک گره

- قوانین زیر برای قضاوت در مورد گره های غیرمعتبر استفاده می شوند:
  - گره ای که تعدادی بسته داده به گره های دیگر ارسال کرده است نمی تواند خرابکار باشد.
  - گره ای که تعداد زیادی داده دریافت کرده و آنها را ارسال نکرده است ممکن است خرابکار باشد.
  - گره خرابکار، گره ای است که حداقل یک RREP فرستاده است.
  - گره ای که تعداد زیادی داده دریافت کرده و آنها را ارسال نکرده است و حداقل یک RREP فرستاده است مطمئناً یک گره خرابکار است.



a) node2 reply to a RREQ packet
b)node1 initiates a judgment process in neighbors of node2
c) Neighbors send their opinion about node2
d) node1 an alarm to network

63/32 محیط شبیه سازی

- روش پیشنهادی با استفاده از glomosim شبیه سازی شده است.
- در شبیه سازی پارامترهای مختلفی برای ارزیابی روش پیشنهادی معرفی شده است، تعدادی از این پارامترها عبارتند :
  - تاخیر بسته های داده: متوسط تاخیر بین زمان ارسال بسته تا زمان دریافت بسته که شامل همه تاخیرهای بوجود آمده مثل مسیربابی، بافرینگ و پردازش در گره های میانی و غیره
  - نرخ تحویل بسته: کل بسته های دریافت شده به کل داده های ارسال شده.
  - نرخ گذردهی گره ها: کل اطلاعات دریافت شده در واحد زمان.
  - سربار الگوریتم: کل بسته های غیرداده ای مثل RREQ و RREP و...
- سه سناریو شبیه سازی شده است.

محیط شبیه سازی

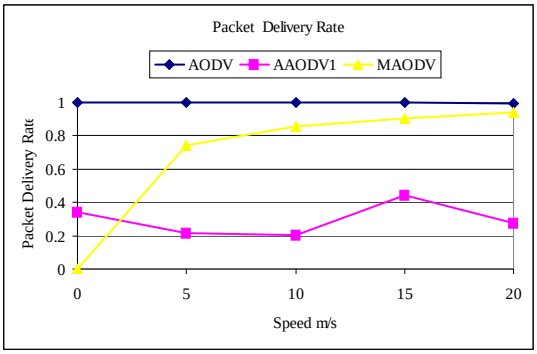
63/33

- در نمودارهای رسم شده سه پروتکل بررسی شده است:
  - AODV : پروتکل AODV پایه می باشد که هیچ گره خرابکاری وجود ندارد.
  - MAODV: روش پیشنهادی برای مقابله با گره های خرابکار می باشد.
  - AAODVn: پروتکل پایه AODV با وجود n گره خرابکار.

زمان شبیه سازی	600 ثانیه
ناحیه شبیه سازی	1000*1000
نوع جابه جایی	RANDOM-WAYPOINT
تعداد گره ها	50

نرخ تحویل داده در سناریو 1

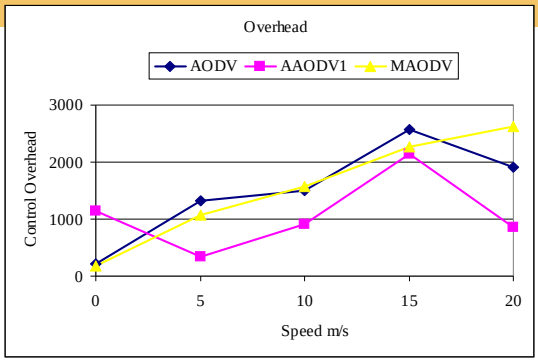
63/34



نتیجه : نرخ تحویل بسته در روش پیشنهادی یا MAODV بسیار نزدیک به AODV می باشد. در حالی که در پروتکل AAODV1 مقدار نرخ تحویل بسته بسیار پائین است. در روش پیشنهادی به دلیل شناسایی گره خرابکار و قرنطینه کردن آن، کارآئی این روش بسیار نزدیک به روش AODV می باشد.

سربار الگوریتم در سناریو 1

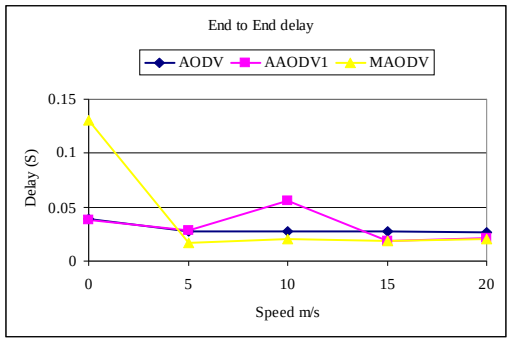
63/35



- نتیجه : روش پیشنهادی به دلیل پخش همگانی درخواست بررسی، دارای سربار اضافی می باشد. اما به دلیل به روز رسانی جدول های مسیریابی، حجم سربار اضافی کاسته می شود. در روش AAODV1 به دلیل اینکه گره خرابکار همواره مسیرها را به منابع پیشنهاد می کند، برای همین دارای سربار کمتری است. البته باید توجه کرد که این پروتکل داده بسیار کمی را به مقصدها تحویل می دهد.

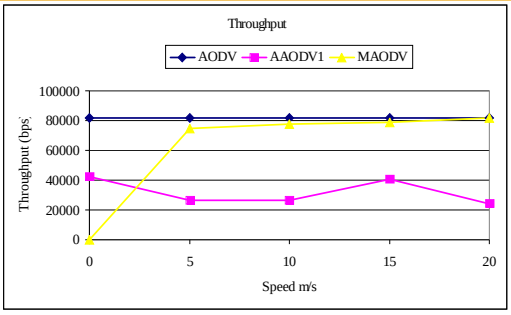
تاخیر در سناریو 1

63/36



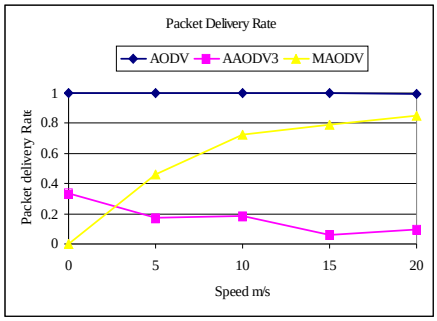
نتیجه : به دلیل اینکه روشAAODV1 دارای کمترین سربار است دارای کمترین تاخیر می باشد و سپس روش پیشنهادی به دلیل ارسال RREQ های سراسری کمتر ، دارای کمترین تاخیر می باشد. در روش پیشنهادی در زمانی که گره ها دارای سرعت پایین می باشند به دلیل اینکه ممکن است مسیرهای بین گره ها به سختی برقرار شود و یا اصلا برقرار نشود RREQ های بیشتری ارسال شود علاوه بر این به دلیل عدم وجود اطلاعات کافی درخواست نظرات نیز به دفعات ارسال خواهد شد و این باعث افزایش تاخیر در ابتدا برای روش ما می شود .

63/37 نرخ گذردهی در سناریو 1



نتیجه : به دلیل اینکه روش پیشنهادی در ابتدا دارای تاخیر بسیار زیاد و سربار زیاد می باشد، تعداد بسته های داده دریافتی بسیار پایین می باشد. اما به تدریج که سرعت بالاتر می رود گره خرابکار شناسایی شده و قرنطینه می شود.

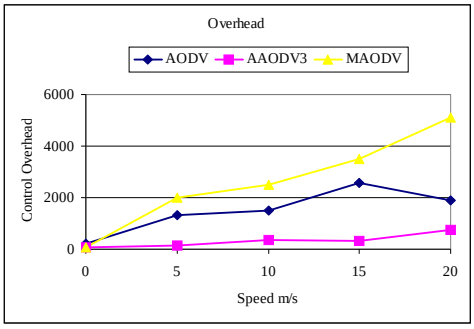
63/38 نرخ تحویل داده در سناریو 2



نتیجه : در روش پیشنهادی به دلیل شناسایی و قرنطینه کردن گره های خرابکار، الگوریتم پیشنهادی دارای نرخ تحویل بسته نزدیک به روش AODV پایه می باشد. اما در روش AAODV1 گره خرابکار تا آخر شبیه سازی اطلاعات را از بین می برد.

سربار الگوریتم در سناریو 2

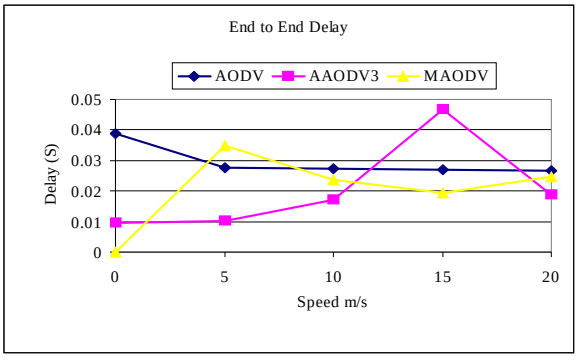
63/39



نتیجه : زمانی که تعداد گره های خرابکار زیاد می شود تعداد ارسال های درخواست نظر نیز افزایش می یابد. در الگوریتم AAODV3 به دلیل اینکه همیشه گره های خرابکار مسیرهای کوتاه را در اختیار گره های فرستنده داده قرار می دهند برای همین سربار آن در مقایسه با دیگر الگوریتم ها بسیار پایین می باشد.

تاخیر در سناریو 2

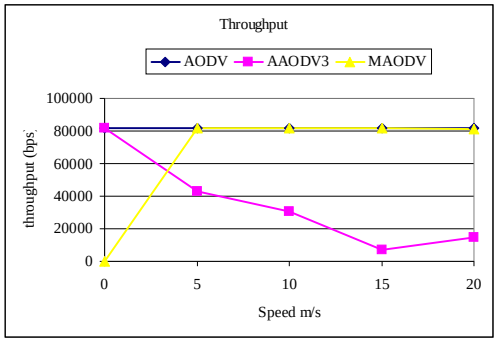
63/40



نتیجه : روش پیشنهادی در ابتدا دارای تاخیر زیادی می باشد اما به تدریج که ندهای خرابکار شناسایی می شوند تاخیر آن دارای یک سیر نزولی منظم مانند AODVپایه می شود.

نرخ گذردهی در سناریو 2

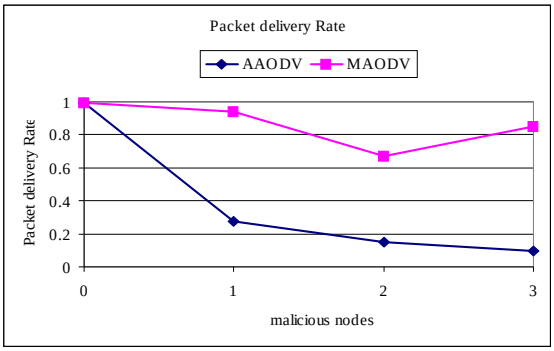
63/41



نتیجه : روش پیشنهادی بلا فاصله با شناسایی گره های خرابکار دارای گذردهی مشابه با الگوریتم پایه می شود. اما در AAODV3 به دلیل عدم شناسایی گره های خرابکار، گره های خرابکار تا آخر شبیه سازی داده ها را دور می ریزند.

نرخ تحویل بسته در سناریو 3

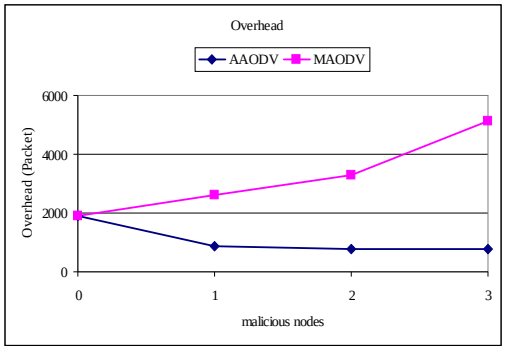
63/42



نتیجه : هرچقدر تعدا گره های خرابکار بیشتر شود سربار الگوریتم بیشتر می شود و همچنین شناسایی گره های خرابکار سخت تر می شود برای همین نرخ تحویل داده با افزایش گره های خرابکار کاهش می یابد.

سربار در سناریو 3

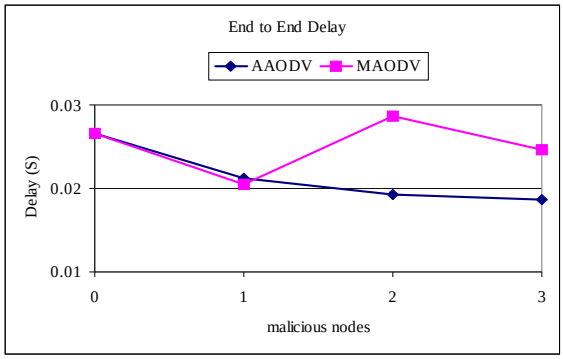
63/43



نتیجه : سربار با افزایش تعداد گره های خرابکار افزایش می یابد زیرا گره های بیشتری، فرایند درخواست نظر یا قضاوت را شروع می کنند برای همین سربار افزایش می یابد.

تاخیر در سناریو 3

63/44



نتیجه : هر چه سربار الگوریتم بیشتر باشد تاخیر آن نیز بیشتر می شود.

نتیجه

63/45

- روش پیشنهادی توانایی تشخیص گره های خرابکار را دارد.
- در زمانی که تعداد گره های خرابکار پایین باشد، با هزینه بسیار اندکی می تواند گره خرابکار را تشخیص دهد.
- به علت پخش همگانی پیغام های درخواست نظر همسایه ها، سربار الگوریتم بالاست اما با به روزرسانی جدول های مسیریابی گره های شبکه، می توان تا اندازه زیادی از سربار الگوریتم کاهش داد.
- از لحاظ پیاده سازی الگوریتم پیشنهادی دارای پیچیدگی خاصی نیست و به راحتی قابل پیاده سازی می باشد.
- ساختار پیغام های جدید معرفی شده بسیار شبیه RREP و RREQ می باشد.

نتیجه - ادامه

63/46

- مزیت های روش پیشنهادی
  - فرایند مسیریابی روند عادی خود را طی می کند و تنها اگر گره پاسخ دهنده گره مشکوک باشد یک فرایند نظرسنجی شروع می شود.
  - در مورد گره های همسایه اطلاعات محدودی نگه داری می شود.
  - گره ها بنا به فعالیت های مثبت خود می توانند در شبکه موجود باشند.
  - گره ای که از خرابکاری مطلع می شود تا حد امکان از خراب شدن اطلاعات با ذخیره آنها جلوگیری می کند.
- مشکلات روش پیشنهادی
  - سربار الگوریتم برای فرایند نظرسنجی
  - اندازه جدول همسایه ها و لیست گره های خرابکار می تواند بزرگ شوند
  - اعلام خرابکار بودن یک گره در شبکه

منابع

63/47

1. H. Deng, W. Li, and D. P. Agrawal, “Routing security in ad hoc networks”, IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
2. S. Lee, B. Han, and M. Shin, “Robust routing in wireless ad hoc networks, ” in ICPP Workshops, pp. 73, 2002.
3. M. A. Shurman, S. M. Yoo, and S. Park, “Black hole attack in wireless ad hoc networks,” in ACM 2nd Southeast Conference (ACMSE’04), pp. 96-97, Apr. 2004.
4. Hesiri Weerasinghe, Huirong Fu, “Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008.
5. Latha Tamilselvan, Dr. V Sankaranarayanan, “Prevention of Co-operative Black Hole Attack in MANET”, JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.

پایان

63/48

با تشکر از حضور و توجه شما عزیزان