مکانیزم های تشخیص خودخواهی گره ها در شبکه های موردی سیار

اکرم شهبازی سیف آباد[۱]،بهرنگ برکتین[۲]

۱- گروه مهندسی کامپیوتر, واحد نجف آباد, دانشگاه آزاداسلامی, نجف آباد, ایران

۲- گروه مهندسی کامپیوتر, واحد نجف آباد,دانشگاه آزاداسلامی, نجف آباد,ایران

خلاصه

شبکه های اقتضایی متحرک، یک شبکه بدون زیر ساخت ودارای قابلیت خود پیکربندی است که از دستگاه های متحرکی که از طریق لینک های بی سیم به هم متصل شده اند، تشکیل شده است. بیشتر پروتکل های شبکه های اقتضایی،بر این فرض استواراند که تمام گره ها در انجام وظایف شبکه همکاری می کنند و روال پیش بینی شده در پروتکل را به درستی و به طور کامل دنبال خواهند کرد در حالیکه ممکن است برخی گره ها به دلایلی نظیر ذخیره باتری، بدست آوردن پهنای باند بیشتر، قصد اخلال در شبکه و غیره همکاری نکنند و به اصطلاح خودخواهی نمایند که این مسئله باعث اخلال در کار پروتکل و در نتیجه کاهش کارایی شبکه خواهد شد.در نتیجه مکانیزمی برای تشخیص و از بین بردن خودخواهی گره ها و مجبور کردن آنها به همکاری، بسیار ضروری است. از این رو دراین تحقیق به بررسی مکانیزم های موجود جهت تشخیص و از بین بردن خودخواهی گره ها و مجبور کردن آنها به همکاری در شبکه های موردی سیار می پردازیم.نتایج حاصل نشان می دهد که تشخیص گره های خودخواه و تحریک آنها به همکاری،سبب افزایش کارایی در شبکه خواهد شد.

کلمات کلیدی: شبکه های اقتضایی متحرک ، پروتکل های مسیریابی،سرویس های امنیتی،گره های خودخواه

۱- مقدمه

انجام وظایف شبکه، نظیر مسیریابی و جلورانی توسط گره ها، برای بهره بردن سایر گره های شبکه، از همکاری گره ها ناشی می شود . بیشتر پروتکل های شبکه های موردی که تاکنون ارائه شده اند بر این فرض استوارند که تمام گره ها در انجام وظایف شبکه همکاری می کنند و روال پیش بینی شده در پروتکل را به درستی و به طور کامل دنبال خواهند کرد[۱]. در حالیکه ممکن است برخی گره ها به

[2]. Corresponding author: Email: behrang_barekatain@iaun.ac.ir

دلایلی نظیر ذخیره باتری، بدست آوردن پهنای باند بیشتر، قصد اخلال در شبکه و غیره همکاری نکنند و به اصطلاح خودخواهی نمایند که این مسئله باعث اخلال در کار پروتکل و در نتیجه کاهش کارایی شبکه خواهد شد[۲].یک گره خودخواه بطور مستقیم قصد وارد کردن خسارت به عملکرد شبکه را ندارد بلکه مایل نیست که منابع خود را برای ارتباطات دیگران مصرف کند. اینگونه گره ها به منظور حفظ منابع خود (پنهای باند، مصرف باتری و Cpu) از پذیرفتن انتقال بسته های گره های دیگر سرباز می زنند و با سایرگره ها همکاری نمیکند که باعث از کار افتادن کل شبکه می شوند.عدم همکاری و خودخواهی از سوی گره ها باعث کاهش شدید کارایی و گذردهی شبکه می شود. آنچه مشخص است این است که اگر راهکاری برای مقابله با گره های خودخواه اندیشیده نشود تمامی گره ها به خودخواهی گرایش پیدا میکنند و پس از مدتی شبکه از کار خواهد افتاد. بنا براین مکانیزمی برای تشخیص و از بین بردن خودخواهی گره ها و مجبور کردن آنها به همکاری بسیار ضروری است. گره خودخواهی، نوعی گره بدرفتار است که از روال تعیین شده در پروتکل تخطی می کند از سوی گره ها, باعث کاهش شدید کارایی و گذردهی شبکه می شود[۳]. آنچه مشخص است این است که اگر راهکاری برای مقابله با گره های خودخواه اندیشیده نشود تمامی گره ها به خودخواهی گرایش پیدا میکنند و پس از مدتی شبکه از کار خواهد افتاد.از این رو در این تحقیق جهت حل مسئله ی وجود گره های خودخواه و کاهش اثر اینگونه گره ها در شبکه های موردی سیار، به بررسی مکانیزم های موجود در این زمینه می پردازیم.

۲- پروتکل‌های مسیریابی در شبکه های موردی سیار

پروتکل‌های مسیریابی بین هر دو گره این شبکه به دلیل اینکه هر گره ای می‌تواند به طور تصادفی حرکت کند و حتی می‌تواند در زمانی از شبکه خارج شده باشد، مشکل می‌باشند. به این معنی که یک مسیری که در یک زمان بهینه‌است, ممکن است چند ثانیه بعد اصلاً این مسیر وجود نداشته باشد.طبقه بندی پروتکل های مسیریابی در شبکه های موردی سیار می تواند به چندین روش انجام شود،اما بسیاری از این روش ها وابسته به استراتژی مسیریابی و ساختار شبکه می باشند.پروتکل های مسیریابی می توانند بصورت مسیریابی مسطح،مسیریابی مبتنی بر موقعیت جغرافیایی و مسیریابی مبتنی بر توپولوژی شبکه گروه بندی شوند. پروتکل های مسیریابی مسطح عبارتنداز[۴و۳]:

۲-۱- پروتکل های مسیریابی مبتنی بر جدول[1]

پروتکل مسیریابی پیشگیرانه با حفظ و نگهداری مسیرهای قبلی از تاخیرهای موجود برای کشف مسیر جلوگیری می کند . این نوع پروتکل مسیریابی تلاش بر آن دارد که در شبکه سازشر برقرار کرده و بروزرسانی اطلاعات مسیریابی هر گره به گره های دیگر در شبکه را

انجام دهد.اطلاعات مسیریابی در تعداد مختلفی از جداول نگهداری می شود و آنها به تغییرات در توپولوژی شبکه توسط پخش جدیدترین سفارشات در شبکه برای برقراری سازگاری در شبکه پاسخ می دهد .درناحیه ای که این پروتکل ها متفاوت هستند ,از طریق اطلاعات مسیریابی بروزرسانی می شوند .ردیابی و نوع اطلاعات در هر جدول مسیریابی نگهداری می شود[۵].

[1] Proactive

۲-۲- پروتکل های مسیریابی مبتنی بر تقاضا[1]

تنها زمانی عمل کشف مسیر را انجام می دهد که گره مقصد ناشناس باشد و هیچ مسیری از قبل وجود نداشته باشد. کل گره ها در شبکه اقتضایی متحرک منابع محدودی مانند پهنای باند و باتری دارند. این پروتکل ها برای کاهش سربار در پروتکل ها،اطلاعات را فقط برای مسیرهای فعال پخش می کنند. زمانی که یک گره برای گره مقصد درخواست مسیر می کند،در ابتدا یک فرآیند کشف مسیر در شبکه رخ می دهد. این فرآیند یک مسیر را با تمام مسیرهای جایگزین دیگر امتحان می کند. یکبار دیگر یک مسیر پابرجا نگهداشته شده و تا زمانی که مسیر خارج از دسترس است،در طول مسیر درخواستی از منبع تا مقصد را دنبال می کند. در فرآیند کشف مسیر معمولاً از طریق پخش سیل آسا[2]یک بسته درخواست مسیر در شبکه اتفاق می افتد. وقتی یک گره با یک مسیر به مقصد رسیده است, یک مسیر پاسخ به گره مبداء با استفاده از لینک برگشتی ارسال می شود[۶].

۲-۳- پروتکل های مسیریابی ترکیبی[3]

ترکیبی از دو پروتکل مسیریابی مبتنی بر جدول و مبتنی بر تقاضا می باشد. این پروتکل‌ها روش مسیریابی بردار-فاصله را برای پیدا کردن کوتاهترین مسیر به کار می‌گیرند و اطلاعات مسیریابی را تنها وقتی تغییری در توپولوژی شبکه وجود دارد را گزارش می‌دهند. هر گره ای در شبکه برای خودش یک zone مسیریابی دارد و رکورد اطلاعات مسیریابی در این zoneها نگهداری می‌شود[۴].
پروتلهای مسیریابی بر اساس پارامترهای کانال مانند تضعیف، انتشار چند مسیره، تداخل و همچنین بسته به کاربرد شبکه به صورت بهینه طراحی شده اند.

۳- سرویس های امنیتی در شبکه های موردی سیار

به منظور اطمینان از انتقال معتبر داده از شبکه های ارتباطاتی جهت حفاظت از منابع سیستم، به چندین سرویس امنیتی نیازمندیم .بر اساس اهداف آنها،سرویسهای امنیتی به پنج دسته تقسیم میشوند[۸, ۷]:

۳-۱- **دردسترس بودن :**[4]نشان می دهد که سرویس های درخواستی به روشی زمانی موجود است حتی اگر مشکل پتانسیل در سیستم موجود
باشد .موجودیت شبکه می تواند از دست برود. مثلاً از طریق افت بسته ها و یا از طریق حمله برمنبع.

۳-۲- **قابلیت اعتماد :**[5]اطمینان می دهد که اطلاعات دسته بندی در شبکه،هرگزبه بخش های ناخواسته فاش نمی شود .اطمینان یابی را می توان از طریق استفاده از تکنیک های نوشتاری مختلف حاصل کرد.حمله

[1] Reactive
[2] Flooding
[3] Hybrid
[4] Availability
[5] *Confidentiality*

۳-۳- افشای محتوا وحمله افشای محل،محتوای پیام در حال ارسال و اطلاعات فیزیکی مربوط به گره های خاص را نشان می دهد.

۳-۴- **سندیت :**[1]سرویس شبکه ای که شناسه ی کاربر را تعیین می کند بدون سندیت(تصدیق)،یک حمله گرمی تواند به هرگره ای دست یافته و از این راه یک به یک گره ها را گرفته و به کل شبکه دست یابد.

۳-۵- **انسجام :**[2]تضمین می کند که اطلاعات که بین گره ها گذر می کنند،در ارسال آسیب نمی بینند. داده می تواند به صورت عمدی یا غیرعمدی تغییر یابد.

۳-۶- **عدم رد سرویس :**[3] تضمین می کند که منشاء اطلاعات نمی تواند ارسال اطلاعات را رد کند.

۴- سوءرفتار[4] گره ها در شبکه های موردی سیار:

یکی از مشکلات عمده شبکه های موردی، پیدا کردن گره ای است که در عملیات مسیریابی شرکت نمی کند و یا قصد تخریب این عمل را دارد. درواقع می توانیم سوء رفتار را از چند دیدگاه دسته بندی کنیم[۴,۹].

۴-۱- **سوء رفتار به صورت تصادفی[5] / عمدی[6]:** بدین معنا که آیا سوء رفتاری که توسط یک گره صورت گرفته است به صورت تصادفی است و یا اینکه خود گره با دانش اینکه رفتار او بر خلاف استراتژی شبکه است، این رفتار را انجام داده است[۴].

۴-۲- **سوء رفتار از دید خودخواه[7] یا خرابکارانه[8]** : سوء رفتارهایی که از روی خودخواهی صورت می پذیرند، به به این علت انجام می شوند که گره خودخواه می خواهد از زیر بار شرکت در عملیات مسیر یابی فرار کند و بدین ترتیب در وقت و به خصوص انرژی خود صرفه جویی نماید. به همین دلیل در این دسته از سوء رفتارها، اغلب بسته های دریافتی توسط گره متخاصم نادیده گرفته می شود و به جلو ارسال نمی گردد. اما در سوء رفتارهای خرابکارانه، گره متخاصم قصد خرابکاری در عملیات مسیریابی و به دست آوردن یک مورد خاص است. بنابراین ممکن است در راستای دستیابی به هدف خود، دست به هر کاری بزند. هرچند که این کار به قیمت مصرف انرژی و وقت زیادی از خود گره تمام بشود[۹].

---
[1] *Authenticity*
[2] Integrity
[3] *Non-repudiation*
[4] misbehavior
[5] Random
[6] Intentional
[7] Selfish
[8] Malicious

۴-۳- سوء رفتار فردی[1]: یک گره به صورت منفرد, اقدام به بدرفتاری در عملیات مسیریابی می کند[۴].

۴-۴- سوء رفتار دسته جمعی: تعدادی از گره ها با کمک یکدیگر اقدام به بدرفتاری در عملیات مسیریابی می کنند. غالباً تشخیص و جلوگیری از سوء رفتارهای دسته جمعی، بسیار سخت تر از نوع فردی آن است[۹].

معمولاً تشخیص یک سوء رفتار از یک رفتار درست در شبکه های موردی کار مشکلی است. زیرا ما تنها چیزی که مشاهده می کنیم رفتار خارجی یک گره است و از اتفاقاتی که درون آن گره می افتد اطلاعی نداریم. به عنوان مثال یک گره می تواند یک بسته را به دلیل رو به اتمام بودن باتری خود و یا به دلیل اشکال در ارسال بسته رها کند و آن را ارسال ننماید.بنابراین نمی توان عدم ارسال یک بسته توسط یک گره را به حساب سوء رفتار آن گره گذاشت.

۵- انواع گره های موجود در شبکه های موردی سیار

در شبکه های موردی سیار ممکن است گره ها ی مختلفی وجود داشته باشد که عبارتند از[۱۰, ۲,۴]:

۵-۱- گره های خوش رفتار: منظورازخوش رفتاری،تبعیت ازروال تعیین شده در پروتکل است و گره ای که رفتار تعیین شده در پروتکل را دنبال می کند،گره خوش رفتار نامیده می شود.

۵-۲- گره های بدرفتار:ممکن است برخی گره ها به دلایلی نظیر ذخیره باتری،بدست آوردن پهنای باند بیشتر،قصداخلال درشبکه و غیره همکاری نکنند وبه اصطلاح" بدرفتاری " نمایند .این مساله باعث

اخلال در کار پروتکل و در نتیجه کاهش کارایی شبکه خواهد شد. منظوراز بدرفتاری،تخطی از روال تعیین شده در پروتکل است و گره ای که رفتار تعیین شده در پروتکل را دنبال نمی کند،گره بدرفتارنامیده می شود[۲].گره های بدرفتارسه نوع می باشند [۱۰, ۲,۴]:

۵-۲-۱- گره بدخواه : به دسته ای از گره های بدرفتارگفته می شودکه گره،عمدا سعی در حمله به سیستم را دارد.اینگونه گره ها بطور مستقیم قصد وارد کردن خسارت به عملکرد شبکه را دارند و سبب ایجاد اختلال در عملکرد شبکه می شوند[۲].

۵-۲-۲- گره خودخواه: به دسته ای از گره های بدرفتارگفته می شودکه گره، بطور مستقیم قصد وارد کردن خسارت به عملکرد شبکه را ندارد بلکه مایل نیست که منابع خود را برای ارتباطات دیگران مصرف کند. اینگونه گره ها به منظور حفظ منابع خود (پنهای باند، مصرف باتری و Cpu) از پذیرفتن انتقال بسته های گره های دیگر سرباز می زنند و با سایرگره ها همکاری نمی کنند. این رفتار گره ها ممکن است باعث از کار افتادن کل شبکه شود[۱۰].

۵-۲-۳- گره خرابکار:گره متخاصم قصد خرابکاری در عملیات مسیریابی و به دست آوردن یک مورد خاص را دارد. گره های متخاصم ممکن است برای مختل کردن عملکرد شبکه ،رفتاری خودسرانه در پیش گیرند .آنها قادر به خراب کردن،

[1]Freddie

اجرای مجدد و همچنین ساختن بسته های مسیریابی می باشند .این گره ها ممکن است به هر روشی در صدد منحرف کردن بسته ها از مسیر خود باشند و عموماً نمی توان توقع داشت که به درستی پروتکل مسیریابی را اجرا کنند[۴] .

۶-انواع سوءرفتار گره های خودخواه

سوءرفتار گره های خودخواه سبب می شود تا اینگونه گره ها به منظور حفظ منابع (پنهای باند، مصرف باتری و Cpu) از پذیرفتن انتقال بسته های گره های دیگر سرباز زنند و با سایرگره ها همکاری نکنند. انواع سوءرفتار گره ها عبارتند از [۴,۱۰]:

۶-۱- هدایت نکردن پیغام درخواست مسیر(RREQ)[1]: وقتی یک گره مبداء نیازمند یک مسیر به سمت گره مقصد باشد و مسیر معتبری در جدول مسیریابی نباشد، گره مبداء یک بسته درخواست مسیر (RREQ) را به سمت گره مقصد همه پخشی می کند. وقتی هر گره RREQ را دریافت می کند، یک ورودی

مسیر برعکس به سمت گره مبداء را در جدول مسیریابی ایجاد یا بروز رسانی می کند و اگر یک مسیر معتبر در جدول مسیریابی به سمت گره مقصد، ندارد، RREQ را دوباره همه پخشی می کند. اگر در این مسیر،گره خودخواهی وجود داشته باشد،در این همه پخشی شرکت نمی کند و از جلورانی این پیغام امتناع می کند[۴] .

۶-۲- هدایت نکردن پیغام داده [2]: پس از آنکه یک مسیر معتبر از گره مبدا به گره مقصد ایجاد شد،آنگاه گره مبدا اقدام به ارسال داده به گره مقصد می کند. اگر در این مسیر ،گره خودخواهی وجود داشته باشد،بسته داده را به سمت جلو هدایت نخواهد کرد[۱۰] .

۶-۳- هدایت نکردن پیغام تائیدیه(ACK)[3] : پس از آنکه گره مقصد بسته ارسالی از گره مبدا را دریافت کرد، یک پیغام تائیدیه(ACK) را به گره مبدا ارسال می کند تا گره مبدا مطلع شود که بسته اش به گره مقصد رسیده است. اگر در این مسیر،گره خودخواهی وجود داشته باشد،بسته داده را به سمت جلو هدایت نخواهد کرد[۴] .

۶-۴- ارسال نکردن پیغام سلام(Hello)[4]: هر نود می تواند از همسایه های خود با استفاده از پخش همگانی محلی اطلاع پیدا کند که به آن پیام های Hello گفته می شود.همسایه های یک نود ، نودهایی هستند که آن می تواند مستقیما با آنها ارتباط برقرار کند . بنابراین AODV یک پروتکل واکنشی است که از این پیام های Hello ای دوره ای استفاده می کند تا همسایه هایی که در این لینک هنوز فعال نیستند را شناسایی کند . پیام های Hello هرگز پیشرو نیستند زیرا آنها با مقدار TTL=1 در شبکه پخش می شوند . زمانی که یک نود ، پیام Hello را دریافت کرد ، طول

[1] Not forwarding Route Request message
[2] Not forwarding Data Messsage
[3] (Not forwarding Acknowledgement Messsage
[4] Not sending Hello Messsage

عمر اطلاعات همسایه را در جدول مسیریابی به روز می کند. هر نود بطور متناوب یک بسته Hello را برای اتصالات محلی همه پخشی کرده و RREP را با TTL=1همانند بسته Hello همه پخشی می کند[۱۰] . اگر گره خودخواهی وجود داشته باشد، از ارسال این پیغام امتناع می کند[۴] .

۶-۵- تاخیر در هدایت پیغام درخواست مسیر(RREQ)[1]: اگر در یک مسیر،گره خودخواهی وجود داشته باشد،ممکن است از ارسال بموقع پیغام درخواست مسیر(RREQ) امتناع بورزد و این پیغام را با تاخیر ارسال کند.[۴] .

۶-۶-هدایت نکردن پیغام پاسخ درخواست مسیر(RREP)[2]: بسته پاسخ(RREP) بصورت تک پخشی با استفاده از مسیر ایجاد شده توسط درخواست مسیر

به سمت گره منبع فرستاده می شود. بنابراین پس از اتمام فرآیند کشف مسیر، بسته می تواند از گره منبع به مقصد و بالعکس ارسال شود.
اگر در این مسیر،گره خودخواهی وجود داشته باشد، از ارسال این پیغام امتناع می کند[۴] .

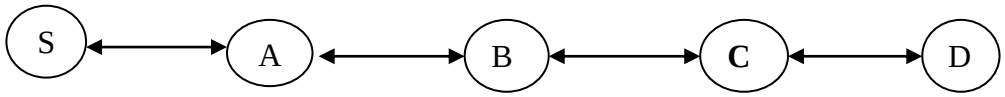
۷- برخی تکنیک های موجود جهت تشخیص گره های خودخواه در شبکه های موردی سیار

حال به چند نمونه از تکنیک های تشخیص و مقابله باگره های خودخواه در شبکه های موردی سیار می پردازیم:

۷-۱-Watchdog

در این تکنیک هرگره ای که اطلاعات مسیریابی را ارسال می کند،نگهبان آن اطلاعات است تا آنها از طریق گره بعدی نیز ارسال شوند. شبکه ارائه شده درشکل۱ را در نظربگیرید .فرض کنید گره S قصد یافتن مسیری به گره D را دارد. هر چند گره A نمیتواند اطلاعات را مستقیما به گره C برساند, ولی می تواند مراقب رفتار گره B باشد تا ببیند که آیا گره B اطلاعات را به گره C ارسال میکند یا خیر .بعلاوه اگر اطلاعات بدون رمز کردن ارسال شود A می تواند از دست نخوردن اطلاعات توسط گره B نیزمطلع شود .حالا اگر گره A از یک بافر برای اطلاعات ارسالی استفاده کند می تواند رفتارهای سوءگره B را تشخیص دهد.بدین ترتیب که A هر بسته ای را که ارسال می کند داخل بافر قرار می دهد. اگر طی زمان مشخصی, پیامی از B برای C صادر نشود,A به شمارنده ای که به این منظور اختصاص داده است یک واحد اضافه می کند. حال اگر تعداد این شمارنده از یک حد آستانه ای بیشتر شد, این اتفاق به عنوان خودخواهی کره B در نظر گرفته می شود [۱۱].

[1] Delayed forwarding Route Request messages
[2] Notforwarding Route Reply message



شکل (۱): شبکه موردی نمونه در تکنیک Watchdog

Pathrater -۲-۷

الگوریتم ارزیاب مسیر برای انتخاب یک مسیر از منبع به مقصد به جای کوتاهترین مسیر از یکالگوریتم رتبه بندی ساده استفاده می نماید. ارزیاب مسیر که توسط هر گره ایجاد می شود، دانش گره های دارای سوء رفتار را با قابلیت اطمینان پیوند شبکه می آمیزد تا مطمئن ترین مسیر را برای ارسال بسته پیدا کند. هر گره نرخ سوء رفتاری را به تمامی گره های داخل شبکه نسبت می دهد. حال در هنگام مسیریابی, پس از به دست آوردن هر مسیر، نرخهای گره های داخل مسیر را با یکدیگر جمع کرده و میانگین می گیرد. بدین ترتیب می تواند مسیری را که دارای بیشترین میزان قابلیت اطمینان است ,انتخاب نماید. اگر ارزیاب مسیر,گره ای را در مسیر خود پیدا کند که در حال بدرفتاری است و هیچ مسیر دیگری بدون گره های بدرفتار وجود نداشته باشد، ارزیاب بسته درخواست مسیر را صادر می کند. این عمل به شرطی است که بسطی به نام ارسال بسته درخواست فعال شده باشد[۱۲].

End-to-end Acknowledgements -۳-۷

این مکانیزم شامل نظارت بر قابلیت اطمینان مسیرها از طریق تائید کردن بسته ها به صورت نقطه به نقطه جهت ارائه یک پروتکل مسیریابی قابل اطمینان می باشد. در این تکنیک, گره مقصد یک تائیدیه دریافت بسته را به گره مبدا ارائه میدهد. این تکنیک کمک می کند تا از ارسال بسته ها از طریق مسیرهای غیر قابل اطمینان اجتناب شود و می تواند با تکنیک های دیگر ترکیب شود. این تکنیک همچنین کمک می کند مسیرهای حاوی گره های خودخواه و خرابکار تشخیص داده شوند اما هیچگونه اطلاعات اضافی راجع به گره ای که مسبب گم شدن بسته ها شده است, ارائه نمی دهد [۱۳].

Credit based system -۴-۷

در سیستم مبتنی بر اعتبار,همه گره ها مقداردهی اولیه اعتبار می شوند و با همه گره ها به طور مساوی رفتار می شود. سپس با توجه به اینکه آیا گره ,بسته ها را هدایت می کند یا خیر, مقدار اعتبار افزایش یا کاهش پیدا می کند.اگر یک بسته به یک گره رسید و آن گره بسته را با موفقیت انتقال داد سپس مقدار اعتبار افزایش پیدا می کند. در غیر اینصورت مقدار اعتبار کاهش پیدا می کند. برای مدت زمان اندکی رفتار گره زیر نظر گرفته می شود. وقتی که مقدار اعتبار کمتر از حد آستانه شد ,آنگاه بسته های بعدی جهت انتقال به آن گره واگذار نمی شود [۱۴].

CONFIDENT[1] -۵-۷

[1] Cooperation of Nodes, Fairness in Dynamic Ad-hoc Networks

اساس کار در این روش ,محاسبه مقدار اعتبار هر گره می باشد.هر وقت مقدار اعتبار برای هر گره خاص از یک حد آستانه از پیش تعیین شده کمتر باشد,پروتکل ,انتقال بسته ها از طریق آن گره را متوقف می کند.در این روش هر گره در شبکه شامل دو لیست می باشد. گره هایی که رفتار منطقی و درستی دارند در لیست Friends و گره هایی که بسته ها را دور می اندازند یا قصد مداخله در شبکه را دارند,در لیست Black نگهداری می شوند. اطلاعات این لیست ها از طریق گره های مجاور مبادله می شوند تا دیگر گره ها از وجود گره های خودخواه مطلع شوند[۱۵].

IDS[1] SYSTEM- ۶-۷

در این روش از یک سیستم تشخیص نفوذ استفاده شده است که میتواند به عنوان یک ابزار, روش یا منبعی برای کمک به تعریف, شناسایی, ارزیابی و گزارش فعالیت های شبکه ی غیر مجاز و یا تائید نشده استفاده شود. ماژول سیستم تشخیص نفوذ از طریق ردیابی رفتار گره های خودخواه اعمال میشود. این ماژول ابتدا بررسی میکند که کدام گره در جدول مسیریابی بروز رسانی شده است. سپس اقدام به ارسال شماره توالی بالاتر به گره ی فرستنده میکند.اگر گره ای پیدا شد انگاه این سیستم پیغامی مبنی بر حذف این مسیر خاص که به گره خودخواه تعلق دارد به گره فرستنده ارسال میکند. ماژول تشخیص نفوذ تنها حفاظت از خودخواهی و جلب اعتماد و ارتباط بین فرستنده و گیرنده را فراهم می کند [۱۶].

MADSN[2]-۷-۷

در این روش,هر گره یک شناسه منحصر به فرد در شبکه دارد.گره مبدا بعد از یک دوره زمانی خاص, یک عامل سیار (MA[3]) را ایجاد می کند.عامل سیار با استفاده از RREQ[4] وRREP[5]به سمت مسیر جلورانی ایجاد شده حرکت می کند.عامل سیار دریافت بسته و جلورانی آنها توسط هر گره را محاسبه می کند.اگر عامل سیار, یک گره خودخواه را کشف کند به جای جلورانی, یک گزارش تهیه و برای گره مبدا ارسال می کند تا گره مبدا را از وجود گره خودخواه مطلع سازد[۱۷].

۸- نتیجه گیری

برخی گره ها به دلایلی نظیر ذخیره باتری، بدست آوردن پهنای باند بیشتر، قصد اخلال در شبکه و غیره همکاری نکنند و به اصطلاح بدرفتاری نمایند که این مسئله باعث اخلال در کار پروتکل و در نتیجه کاهش کارایی شبکه خواهد شد. . در نتیجه مکانیزمی برای تشخیص و از بین بردن بدرفتاری گره ها و مجبور کردن آنها به

همکاری بسیار ضروری است. از این رو دراین تحقیق به بررسی مکانیزم های موجود جهت تشخیص و از بین بردن خودخواهی گره ها و مجبور کردن آنها به همکاری در شبکه های موردی سیار پرداختیم. نتایج نشان می دهد که تشخیص گره های خودخواه و تحریک آنها به همکاری,سبب افزایش کارایی شبکه خواهد شد.

[1] Intrusion Detection System
[2] Selfish NodeMobile Agent Based Detection of
[3] Mobile Agent
[4] Route Request message
[5] Route Reply message

منابع

1. K.Sridevi, S.Kannan, S.Karthik.(2012),“A Survey on Selfish Node Detection Using Several Techniques in MANET,”International Journal of Inventive Engineering and Sciences (IJIES) ,pp1018-1022.

۲. سجاد پیراهش ,مسعودصبایی و سعیدسلطانعلی.(۱۳۸۶) ، "ارائه روشی ترکیبی برای بهبود همکاری درشبکه های موردی سیار،"سیزدهمین کنفرانس ملی انجمن کامپیوتر، جزیره کیش،ایران،۲۱-۱۹ اسفند،۲۰۳- .۱۹۵

3.F.De Rango, F.Guerriero, P.Fazio.(2012),“Link-Stability and Energy Aware Routing Protocol in Distributed Wireless Networks,” IEEE Journals & Magazines, Vol. 23, No. 4, pp.713-726.

۴. بهرام نجف پور(۹۱) ، "امنیت مسیریابی در شبکه های موردی سیار،"سمینارکارشناسیارشد،دانشگاه آزاد اسلامی واحدعلوم تحقیقات،تهران.

5.Xia, Z.Jia, L.Ju.(2011), “Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory”, IET Journals & Magazines, Vol. 1, No. 4, pp-1709-266.

6.M.Lima, A.dos santos, G.Pujolle.(2009), “ A Survey of Survivability in Mobile Ad Hoc Networks”, IET Journals & Magazines, Vol. 11, No. 1, pp.66-77.

7. N.Shanthi, DR.Lganesan, DR.K.ramar.(2009), “ STUDY OF DIFFERENT ATTACKS ON MULTICAST MOBILE AD HOC NETWORK”, Journal of Theoretical and Applied Information Technology- JATIT.

8.S.Kumar, G.Pruthi, A.Yadav, M.Singala.(2012, “ Security Protocols in MANETs”,IEEE Conference, pp.530-534.

9. Liana Khamis Qabajeh, Dr. Miss Laiha Mat Kiah, Mohammad Moustafa Qabajeh.(2009) ,“ A Qualitative Comparison of Position-Based Routing Protocols for Ad-Hoc Networks”, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2.

10. Debjit Das, Koushik Majumder and Anurag Dasgupta.(2015) ,“ Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory”, Eleventh International Multi-Conference on Information Processing (IMCIP), pp92 – 101.

11. DipaliKoshti, SupriyaKamoji.(2011), “ Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks”, International Journal of SoftComputing and Engineering (IJSCE), Volume-1, Issue-4.

12. SagarPadiya, Rakesh Pandit&Sachin Patel.(2013), “ Survey Of Innovated Techniques To Detect Selfish NodesInMANET”,International Journal Of Computer NetworkingWireless And Mobile Communications (IJCNWMC) Vol. 3, Issue 1.

13. Sumiti, sumit Mittal.(2015), “ Identification Technique for all passive selfish node attacks in mobile network”, International journal of advanced research in science &

computer management studies Volume 3, issue 4.
14. Alberto Rodriguez-Mayol and Javier Gozalvez.(2010), " Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks", Conference paper.
15.J.Vijithanand, K.Sreeramamurthy.(2012),"A survey on finding selfish nodes in mobile ad hoc networks," international journal of computer science and information technologies, vol. 3
16. Gaurav Soni1 and Kamlesh Chandrawanshi.(2013),"A NOVEL DEFENCE SCHEME AGAINST SELFISH NODE ATTACK IN MANET,"International Journal on Computational Sciences & Applications (IJCSA) Vol.3, No.3, pp.51-63.
17.Debdutta Barman Roy and Rituparna Chaki.(2011), "Mobile Agent Based Detection of Selfish Node in MANET,"International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4,pp225-235.
18. Anujk. Gupta, Harsh. S., Anil K. Verma.(2011),"A Review of Routing Protocols for Mobile Ad Hoc Networks", Volume. 10, NO. 11.