مسیریابی مبتنی بر اعتماد در شبکه های حسگر بی سیم با استفاده از منطق فازی

حسین مومن زاده [۱] ، فاطمه باوی [۲] ، مسعود اعتصامی [۳]

۱: دانشگاه آزاد اسلامی، واحد بوشهر ، گروه برق بوشهر ، ایران ، Momenzadeh.hossein@gmail.com
۲: دانشگاه آزاد اسلامی، واحد بوشهر ، گروه کامپیوتر بوشهر ، ایران ، Fatemehbavi@yahoo.com
۳: دانشگاه آزاد واحد گناوه ، گروه ریاضی گناوه ، ایران Etesami.masoud@yahoo.com
تاریخ دریافت: ۱۳۹۵/۷/۲۴ تاریخ پذیرش: ۱۳۹۶/۴/۲۱

چکیده

شبکه‌های حسگر بی‌سیم، حوزه‌ی پرکاربردی از نسل‌های شبکه با پتانسیل بالا در محیط‌های غیرقابل پیش‌بینی و پویا است. با این حال، این شبکه‌ها به دلیل رسانه‌ی باز خود، توپولوژی در حال تغییر و پویا و الگوریتم‌های مسیریابی آن آسیب‌پذیر است . شبکه‌های موردی و شبکه‌های بی‌سیم ویژگی‌های مختلف مثل خود سازمان‌دهی پویا، خود پیکربندی، خود تصحیحی، نگه‌داری آسان، مقیاس‌پذیری بالا و سرویس‌های مطمئن را پشتیبانی می‌کند علیرغم ویژگی‌های بسیاری که ذکر شد، این شبکه بسیار در برابر خرابی ناشی از حملات مستعد است. عدم وجود یک سیستم کنترل مرکزی شاید مهمترین دلیل این ضعف شناخته شود. همچنین همبندی پویای شبکه امکان پیاده سازی مکانیسم‌های سلسله مراتبی امنیتی را از طراحان شبکه سلب می نماید..توسط راهکار های مبتنی بر اعتماد روشی را پیشنهاد می دهم که بتواند در برابر حملات تغییر ماهیت گره شبکه که به نوعی خطرناکترین حمله نیز در این حوزه محسوب می‌شود مقابله و شبکه را بازیابی کنم.از ویژگی‌های بارز این روش، سربار محاسباتی و اتلاف انرژی ناچیز از یک‌سو و مقابله و ترمیم آثار حملات صورت گرفته در شبکه است. راهکار و مکانیسم پیشنهادی با استفاده از نرم‌افزار شبیه‌ساز NS2 مورد ارزیابی قرارگرفته است. درصد خطای پایین روش پیشنهادی در تعیین میزان اعتماد یک گره در شبکه نکته بارز این مقاله است که توانسته است پس از بروز حمله گره‌های مخرب را تشخیص داده و با قرنطینه سازی آن‌ها از ادامه فعالیت آن‌ها جلوگیری کند.

کلید واژه : معیارهای اعتماد ، پروتکل مبتنی بر اعتماد ، شبکه‌های حسگر

۱- مقدمه

تکنیک‌ها و شیوه‌های مورداستفاده در شبکه‌های حسگر، وابستگی شدیدی به ماهیت کاربرد، ساختار توپولوژی شبکه، شرایط جوی و محیطی، محدودیت‌ها و پارامترهای کارایی و هزینه‌دارند. لذا امروزه در سرتاسر دانشگاه‌های معتبر و مراکز تحقیقاتی کامپیوتری، الکترونیکی و مخابراتی، شبکه‌های حسگر بی‌سیم یک فیلد تحقیقاتی بسیار جذاب و پرطرفدار محسوب می‌شود.

هدف اصلی تمامی این تلاش‌ها و ارائه راهکارها، داشتن سیستمی با شیوه‌های کنترلی ساده، آسان و با هزینه پایین هست که درنهایت با پاسخگویی به نیازمندی‌های مدنظر بتواند در مقابل محدودیت‌ها (پهنای باند، انرژی، دخالت‌های محیطی و ...) ایستادگی کند و شرایط کلی را طبق خواسته‌ها و تمایلات موجود (انتقال حجم زیاد اطلاعات پرمحتوا، بقاء پذیری، امنیت و طول‌عمر بالا، هزینه پائین و ...) فراهم سازد. از مباحث موجود و مهم در شبکه‌های حسگر، بحث مسیریابی و شیوه‌های انتقال و تبادل اطلاعات بین گره‌های شبکه است که وابستگی شدیدی به محدودیت‌ها، منابع موجود و امکانات فراهم‌شده از لایه‌های دیگر شبکه دارد لذا انتخاب الگوریتم مناسب مسیریابی با ماهیت و شرایط کاری شبکه مدنظر، تأثیر به سزایی بر روی پارامترهای ارزیابی کارایی شبکه و همچنین بر میزان هزینه آن دارد، چراکه بایستی اصول تعریفی و ساختاریافته مربوط به شبکه مدنظر رعایت شود. تاکنون راهکارهای متنوعی در این خصوص ارائه‌شده است،[۱۰-۱۳] اما پیش از انجام فرآیند مسیریابی در شبکه‌های حسگر موضوع مهم ایجاد یک مسیر امن جهت ردوبدل شدن داده‌ها احساس شده است. یکی از ابزارهای مورداستفاده برای ایجاد یک مسیریابی امن در شبکه‌های حسگر مکانیسم اعتماد است و ما در این

مقاله از آن استفاده خواهم کرد. مدل‌های اعتماد و اعتبار ابزار مهمی هستند که در بسیاری از زمینه‌ها مانند اجتماعی، اقتصادی و علوم کامپیوتر مورداستفاده قرار می‌گیرند.

مدل‌های اعتماد نقش مهمی برای تصمیم‌گیری در مورد اینکه چه کسی و چگونه در شبکه‌های مختلف عکس‌العمل نشان دهد، دارند. در محیط بدون زیرساخت شبکه‌های حسگر، که به‌صورت موقتی شکل می‌گیرند و توسط خود گره‌ها سازمان‌دهی می‌شوند گره‌های بدخواه به‌خوبی تغییر شکل می‌دهند و می‌توانند با استفاده از خصوصیت ذاتی مشارکت گره‌ها در فرآیندهای شبکه حسگر به عناصر شبکه حمله کنند. به‌عنوان‌مثال تهدیدات امنیتی مانند استراق سمع، کرم‌چاله، رفتار نوسانی و سیاه‌چاله و.... در شبکه‌های حسگر از این دسته هستند که به‌طور ویژه، فرآیندهای مسیریابی را هدف قرار می‌دهند. وجود چنین خصوصیاتی در شبکه حسگر سبب ناپایداری این شبکه‌ها می‌گردد. بنابراین چگونگی انتخاب گره‌های همکار در تراکنش‌ها و فرآیندهای مسیریابی برای افزایش بازده این شبکه‌ها اهمیت زیادی پیدا می‌کند[۱]. سیستم‌های اعتماد روش مفیدی برای تشخیص تهدیدات اعضای فریبکار یا اعضای درخطر افتاده یک شبکه هستند[۲].

بااینکه روش‌های مبتنی بر کلید می‌توانند برای حفظ صحت داده به کار روند و رمزنگاری و روش‌های قدرتمند احراز اصالت ابزارهای قدرتمندی برای حفاظت از صحت بسته‌ها و اعتبار گره‌ها هستند، بااین‌حال قدرت سیستم مدیریت اعتماد بیشتر از روش‌های رمزنگاری و روش‌های احراز اصالت است زیرا این روش‌ها علاوه بر اینکه پیاده‌سازی آن‌ها در شبکه حسگر به دلیل محدودیت‌هایی که دارند مشکل‌ساز است آن‌ها قادر به تشخیص مجموعه بزرگی از حملات مسیریابی مانند رفتارهای خودخواهانه، ارسال انتخابی، سیاه‌چاله، حملات بدگویی و... نیز نیستند. ازاین‌رو می‌توان گفت که برای داشتن کاربردهای امن و قابل‌اطمینان در شبکه‌های حسگر به مدیریت اعتماد نیازمند هستیم[۳].

۲- کارهای مرتبط انجام شده

در [۴] برای امن کردن پروتکل مسیریابی DSR، یک مکانیسم شامل ماژول‌های "watchdog" و"Path rater" طراحی شده است و در پروتکل مسیریابی قرار گرفته است. این روش در پروتکل‌های مسیریابی که در آن‌ها مبدا، مسیر عبوری بسته‌ها را تعیین می‌کند، قابل استفاده است. روش مدیریت اعتماد(منظور روش پیشنهادی) ، یک سیستم اعتبار (Reputation) را به روش watchdog و Path rater اضافه می‌کند . سیستم اعتبار یک لیست سیاه را در هر یک از گره‌ها نگهداری می‌کند و آن را با گره‌های موجود در لیست دوستان به اشتراک می‌گذارد. پروتکلی شبیه به CONFIDANT است، با این حال ازیک سیستم تبادل شهرت پیچیده استفاده می‌کند. هسته شهرت یک گره را به سه مولفه مجزا تقسیم می‌کند. شهرت مستقیم که از طریق مشاهدات شخصی به دست می‌آید، شهرت غیر مستقیم که یک گزارش مثبت به وسیله یک گره دیگر است و شهرت عملیاتی که بر مبنای رفتار مانیتور شده در طول یک کار خاص است. این مقادیر شهرت برای بدست آوردن شهرت کل در یک حالت وزن دار با هم ترکیب می‌شوند. پروتکل TEAODV یک پروتکل مسیریابی مبتنی بر اعتماد آگاه از انرژی است که با افزودن اعتماد به پروتکل مسیریابی آگاه از انرژی EAODV ایجاد شده است. این پروتکل بسیار شبیه به پروتکل Trusted AODV است با این تفاوت که در آن به جای AODV از EAODV استفاده شده است. در این پروتکل از دو مقدار اعتماد استفاده می‌شود، که عبارت‌اند از اعتماد مسیر و اعتماد گره. اعتماد مسیر به وسیله هر گره، برای هر مسیر در جدول مسیریابی‌اش محاسبه می‌شود و در واقع میزان اعتماد به این است که یک بسته می‌تواند به مقصد برسد. پارامتر تحرک و تغییر مداوم همسایگان گره جزء چالش‌های اساسی این پروتکل محسوب می شود. اعتماد گره بر اساس تفاوت بین مقادیر اعتماد اعلام شده گره‌ها به مقصد و میزان اعتماد مشاهده شده برای انتقال داده جاری محاسبه می‌شود. سپس از این مقادیر در تصمیمات مسیریابی استفاده می‌کند.

پروتکل TARF مسیریابی شبکه حسگر را در مقابل مزاحمان منحرف کننده مسیریابی چندگامی با ارزیابی اهمیت گره‌های همسایه انجام می‌دهد. این پروتکل سه پارامتر مهم دارد به نام‌های همسایه (N) که در یک گامی گره است و معیار سطح اعتماد (T) که عددی بین ۰ تا ۱ است و نشان دهنده نظر گره N درباره قابلیت اعتماد گره است، و هزینه انرژی (E) که متوسط مصرف انرژی برای ارسال به گره همسایه است. این پروتکل یک روش تکرار شونده دارد که در ابتدا ایستگاه پایه پیامی را که شامل تعدادی بسته متوالی است ارسال می‌کند. وقتی گره‌ای این پیام را دریافت می‌کند، آخرین دوره و دوره شروع شده را میشناسد. هر بسته ای دربردارنده اطلاعات گره

فرستنده و اطلاعات دوره های طی شده است. سپس احتمال تحویل موفقیت آمیز بسته محاسبه می‌شود و بعد از هر ارسالی کنترلر انرژی سطح انرژی ها را به روز می کند و در صورت تحویل گره عدد، ۱ و در غیر این صورت صفر ذخیره می شود. هر گره ای یک مدیر اعتماد دارد که تصمیم میگیرد که سطح اعتماد هر گره همسایه براساس رخدادهای کشف حلقه، ارسال از ایستگاه پایه و غیره چقدر باشد. در ابتدا همه گره مقدار اطمینان ۰,۵ دارند و بعد از اینکه هر یک از این رخدادها اتفاق افتادند، سطح اعتماد آن گره به روز می‌شود[۵]. در[۴] یک پروتکل مسیریابی برای اجتناب از مکان‌های ناامن ارائه شده است. این پروتکل بر مبنای فرضیاتی است که حسگرها موقعیت تقریبیشان را می‌دانند و در آن از مسیریابی جغرافیایی استفاده می‌کند. در این پروتکل مسیریابی مجموعه‌ای از پروتکل‌های امنیتی بهینه شده برای شبکه‌های حسگر جهت ایجاد محرمانگی داده، احراز هویت دو طرفه و اثبات محرمانگی داده استفاده شده است. با این حال در رابطه با حملات انکار سرویس یا گره‌های به خطر افتاده کار خاصی انجام نمی‌دهد و فقط اطمینان حاصل می‌کند که یک گره به خطر افتاده کلیدهای شبکه را فاش نمی‌کند. در [۶] یک پروتکل مسیریابی امن بر حسب تقاضا در شبکه‌های موردی ارائه شده است که از دستکاری مسیرهای سالم، شامل گره‌های سالم، به وسیله مهاجمین یا گره‌های به خطر افتاده و همچنین از تعداد زیادی از انواع حملات منع سرویس جلوگیری می‌کند . این پروتکل کاراست و فقط از اصول رمزنگاری متقارن با کارایی بالا استفاده می‌کند.

اما در روش پیشنهادی که بر روی پروتکل مبتنی بر روش مسیریابی پویا پیاده‌سازی خواهد شد، معیار اعتماد در شبکه نیز درنظر گرفته می‌شود. با توجه به قابلیت‌های پروتکل پایه من ، بسته جدیدی را تولید نمی‌کنم. بلکه با استفاده از ساختار موجود، روش‌ها و فرمول‌های آماری را در نظر می‌گیریم که با استفاده از آن‌ها و برخی پارامترهای موجود در جداول مسیریابی سعی در تخمین میزان اعتماد به هر گره و مسیر را دارم. با نظر به اینکه انتخاب ما به گونه‌ای است که ابزارهای لازم جهت پیاده‌سازی مکانیزم اعتماد در شبکه در خود پروتکل پایه موجود است. (زیرا پروتکل پایه ما پروتکل AODV می باشد)ز این رو نسبت به کارهای قبلی از سربار شبکه بسیار کمتری برخوردار خواهد بود. بنابراین با وجود سربار پائین و بار محاسباتی کم، انتظار می‌رود انرژی مصرفی شبکه نسبت به پروتکل‌های مرتبط پیشین بهینه‌تر باشد.

هدف از این مقاله مطالعه توانایی روش اعتماد جهت حل مسائل مختلف مطرح در شبکه‌های حسگر و ارائه راهکاری مبتنی بر این روش اعتماد به‌منظور نشان دادن این توانایی است. نحوه استفاده از روش اعتماد باید به‌گونه‌ای باشد که شرایط و محدودیت‌های این‌گونه شبکه‌ها را در نظر بگیرد. در مبحث مسیریابی، هدف ارائه پروتکلی است که علاوه بر امن بودن و قابلیت تحمل‌پذیری در برابر حملات، بتواند طول‌عمر شبکه حسگر را تا حد ممکن افزایش دهد.

۳- روش اعتماد پیشنهاد شده

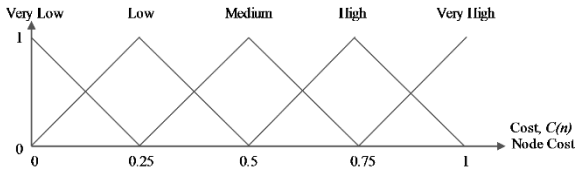
درروش پی شنهادی هدف ت شخیص و مقابله با گره‌ای ا ست که مدام بین رفتار خوب و بد سوئیچ می‌کند. در حالت خوب همانند سایر گره‌های شبکه در مسیریابی‌ها شرکت کرده و نسبت به انتقال بسته‌های مسیریابی و هدایت آن‌ها اقدام می‌کند. اما در حالت بد بسته‌های مسیریابی را جذب کرده و نسبت به حذف آن‌ها وارد عمل می‌شوند. در حالت خوب مشکلی برای شبکه به وجود نمی‌آید. اما در حالت بد تمامی بسته‌های اطلاعاتی شبکه که گره مذکور در مسیریابی آن‌ها شرکت دارد ، از بین میروند . مشکل اساسی تشخیص زمان خوب یا بد بودن رفتار گره مخرب ا ست. برای اینکه بتوانیم این فرآیند را ت شخیص و به‌موقع با آن برخورد کنیم از یک مکانی سم اعتماد چند سطحی استفاده کرده‌ایم. درروش مذکور میزان اعتماد یک گره در گذشته و حال محاسبه شده و از برآیند آن‌ها برای آینده آن گره تصمیم‌گیری می‌شود.

میزان اعتماد یک گره از تابع فازی پی شنهادی حا صل می شود که خود تاثیر پذیر از سه پارامتر دیگر ا ست که این سه پارامتر شامل: نسبت سوئیچ کردن گره، میزان تاخیر انتها به انتهای مسیری که گره مذکور در آن شرکت داشته و اختلاف زمانی اکنون و زمان آخرین تراکنش گره ا ست. در مرحله بعد این میزان اعتماد به‌عنوان اعتماد گذ شته شناخته می شود. دلیل ا ستفاده از نسبت سوئیچ کردن و اختلاف زمانی در این روش این است که چون یکی از معیارهای انتخاب ما همین شرکت کردن یک گره در مسیریابی‌هاست، اگر گره‌ای در مسیریابی شرکت داشته باشد یا فاصله کمی تا مقصد داشته، یا مسیر بهتری را می‌شناسد و یا اعتماد و اعتبار بالاتری دارد. استفاده از گره‌هایی که خیلی قبل در مسیریابی شرکت دا شته‌اند نشان می‌دهد که این سه ویژگی را ندا شته ا ست. اما به جز سه پارامترفوق،

پارامتر دیگری چون حداقل گام تا مقصد نیز می‌توانست ملاک کار قرار گیرد که بدلیل پیچیدگی الگوریتمیک و زمان مورد نیاز جهت همسان سازی بالا استفاده نشد. بنابراین بحث تأخیر انتها به انتها را به‌عنوان دومین ورودی تابع فازی در نظر گرفته‌ایم تا هم اعتماد را درروش کلی دخیل کنیم و هم اعتبار یک مسیر را که گره مذکور در آن قرار دارد. بین گره مبدأ و مقصد ممکن است چندین مسیر وجود داشته باشد. اما پیدا کردن مسیر بهینه خود امری پیچیده است، زیرا مسیر انتخابی باید ازلحاظ ترافیک نیز سربار زیادی نداشته باشد. ممکن است یک مسیر کوتاه بوده و گره‌های آن اعتماد بالایی را داشته باشند اما انتخاب همواره آن توسط گره‌ها می‌تواند باعث ازدحام گشته و موجب افزایش نرخ از دست رفتن بسته‌ها شود. میزان تأخیر انتها به انتها یکی از پارامترهای کیفیت خدمات مسیریابی در شبکه است. هرقدر این تأخیر بالاتر باشد نشان‌دهنده شلوغ بودن مسیر است و مدت‌زمان قرارگیری بسته‌ها در صف گره‌های واسط بالاست[۷].

اختلاف‌زمانی اکنون و زمان آخرین تراکنش گره یک بازه زمانی است. ما از ۱۰ ثانیه استفاده کرده‌ایم. این نمونه‌برداری نباید خیلی کوتاه باشد تا دچار تغییرات لحظه‌ای شبکه نشود و نه خیلی طولانی که نتایج کلی به نظر آیند. لذا این زمان نمونه‌برداری را به‌دلخواه و با توجه به نیاز شبکه متغیر در نظر می‌گیریم. در خصوص زمان شبیه‌سازی نیز چون از شبیه‌ساز NS2 استفاده کرده‌ایم و NS2 از گونه شبیه سازهای رویدادگردان است و از طریق پیگیری رخدادها درطول زمان های گسسته، شبیه سازی را پیش میبرد. این شبیه ساز در دو محیط برنامه نویسی C++ و OTCL و به‌صورت شئ گرا طرح شده است. ورودی های ما سه عنصر تعداد سوییچ ، تاخیر و اختلاف زمان میباشد.

همان‌طور که از منطق فازی و مدل مثلثی برمی‌آید، هر پارامتر ورودی سیستم فازی شامل یک نمودار مثلث‌بندی است. در هر نمودار با توجه به مثلث‌های مشخص و یکسان می‌توان به رفتار یک پارامتر در مقادیر متغیر محور x مقادیری دیگر را در محور y نسبت داد. هر نقطه از محور x دارای دو مقدار در محور y است (شکل۱).



شکل ۱: نمودار تعداد سوئیچ کردن های گره به حالت خوب و بد

و اگر گره ما دارای switch = 0.6، Delay=0.3 ، Time Defrence=5.2، نتایج حاصل از گره ورودی :

Switch=0.6	Delay=0.3	Time Diff=5.2
Medium=0.7	Medium=0.4	High=0.2
High=0.3	Low=0.6	Medium=0.8

که قوانین استخراج شده با توجه به گره ورودی بصورت جدول ۱ می باشد. با توجه به معادله زیر پس از جاگذاری به شرایط عددی زیر خواهیم رسید:

$$NC = \frac{\sum(Rule_i \times C_i)}{\sum(Rule_i)} \qquad (۱)$$

$$NC = \frac{0.346}{1} = 0.346$$

میزان اعتماد گره با توجه به ورودی‌های ما برای این گره برابر 0.346 است.

۴- شبیه‌سازی، ارزیابی و مقایسه روش پیشنهادی

در مسیریابی مبتنی بر اعتماد، چندین حالت مختلف را می‌توان در نظر گرفت. اعتماد گره به گره، اعتماد گره به لینک و بلعکس از مواردی بوده که در شبکه‌های بی سیم قابل پیاده سازی است. ضمناً هرکدام از این روش‌ها می‌تواند بطور غیر مستقیم نیز پیاده سازی

شود بطوری که یک گره از طریق رخدادهای شبکه و دریافت گزار شات هم سایگان میزان اعتماد خود به گره هم سایه را پیش‌بینی و ارزیابی نماید. از این رو راه حل‌های گوناگونی را می‌توان جهت پیاده سازی مکانیسم اعتماد شبکه در نظر گرفت. که ما درروش پیشنهادی به‌صورت ترکیبی از منطق فازی جهت تخمین و اعطای درجه اعتماد گره‌های شبکه بهره برده‌ایم. اما همواره ترکیبی از اعتبار (منظور از اعتبار همان کیفیت لینکی است که شامل تعدادی گره معتمد است.) یعنی ما معیار اعتماد نهایی را وابسته به پارامترهای م سیریابی شامل تاخیر و میزان د ستر سی به گره کرده ایم. بنابر این این گره و گره‌های بعدی در لینک ایجاد شده دارای اعتبار است.)و اعتماد در شبکه می‌تواند مفید باشد. زیرا اگر تصمیم مناسبی در خصوص همسایه نامعتبر یا نامعتمد داشته باشیم شبکه ممکن است به شکست لینک یا ارتباطات ناحیه‌ای منجر شود. در این مقاله ما شبیه‌سازی خود را بر روی پروتکل مسیریابی پایه AODV قرارداده‌ایم. این شبیه‌سازی در محیط NS2.34 پیاده سازی شده و نتایج شبیه‌سازی در ادامه این فصل به ترتیب نوع آزمون آورده شده است (در تمامی شکل ها پروتکل پیشنهادی FLTAODV نامیده شده است).

جدول ۱: قوانین فازی پیشنهادی برای مقدار سوئیچ کردن گره

Antecedent			Consequent
Switch $S_{R(n)}$	Delay $D_{E2E(n)}$	Time Difference $TD_{(n)}$	Node Cost $NC_{(n)}$
High	Very low	Very Low	Very High
High	Low	Very Low	Very High
High	Medium	Very Low	High
High	High	Very Low	Medium
High	Very high	Very Low	Low
High	Very low	Low	Very High
High	Low	Low	Very High
High	Medium	Low	High
High	High	Low	Medium
High	Very igh	Low	Low
High	Very ow	Medium	Very High

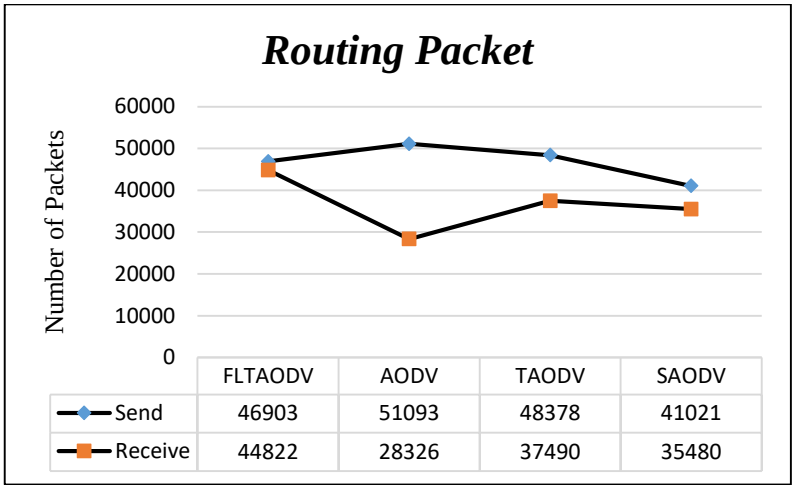
۴-۱ آزمون تعداد بسته‌های مسیریابی

این پارامتر جهت ارزیابی پروتکل پیشنهادی با پروتکل‌های همردیف خود در نرخ مسیریابی بسته‌های شبکه انجام شده است. آزمون مذکور نشان‌دهنده تعداد بسته‌های ارسالی و دریافتی بوده تا بتوان از این ارزیابی به این نتیجه رسید که پروتکل تا چه حد توانسته است بسته‌های تولید شده در شبکه را سالم به مقصد تحویل دهد. معمولاً هر چقدر فاصله تعداد بسته‌های ارسالی و دریافتی به یکدیگر نزدیک‌تر باشد روند پروتکل مناسب‌تر خواهد بود (شکل ۲).

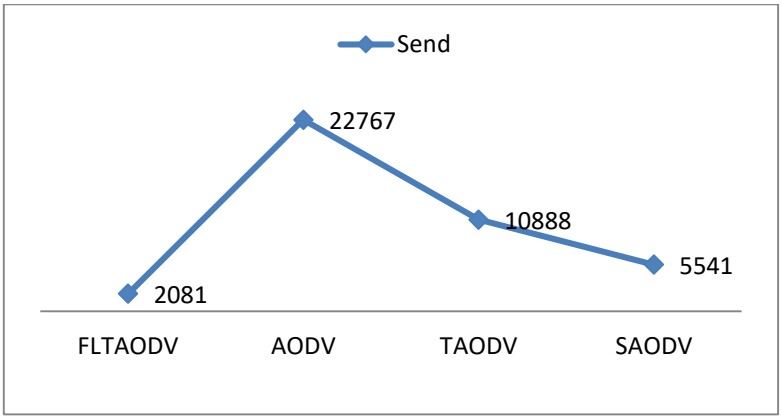
چون یکی از معیارهای انتخاب ما همین شرکت کردن یک گره در مسیریابی هاست، اگر گره ای در مسیریابی شرکت داشته باشد یا فاصله کمی تا مقصد داشته، یا مسیر بهتری را می شناسد و یا اعتماد و اعتبار بالاتری دارد. و در aodv درخواست به همه همسایه ها ارسال میشود.

۴-۲ آزمون تعداد بسته‌های از دست رفته

در مسیریابی شبکه هر قدر فرآیند مسیریابی در انتقال بسته‌های اطلاعاتی موفق عمل کند تعداد بسته‌های از دست رفته در شبیه‌سازی کاهش خواهد یافت (شکل ۳).



شکل ۲: نمودار تعداد بسته های مسیریابی در زمان ۱۰۰۰ ثانیه



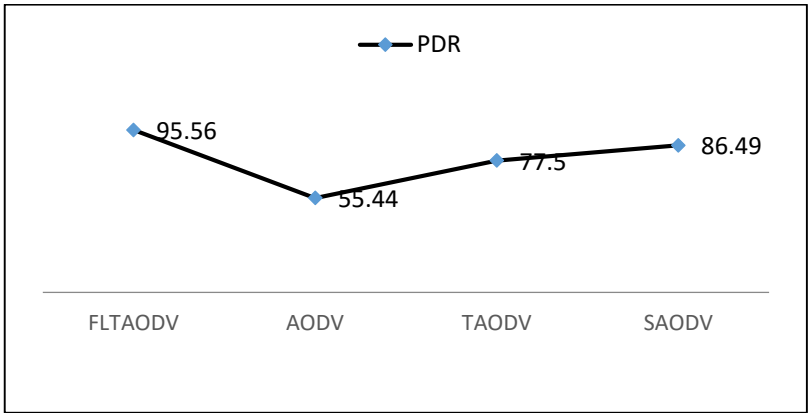
شکل ۳: نمودار تعداد بسته های مسیریابی از دست رفته در زمان ۱۰۰۰ ثانیه: با استفاده از اعتماد سه سطحی وانتخاب بسته های با اعتماد بالاتر حداقل از دست دادن بسته را داریم

۴-۳ آزمون نرخ تحویل بسته ها

این مقدار بر حسب درصد و بر اساس فرمول زیر محاسبه می‌گردد:

$$\mathrm{PDR} = \frac{\sum \text{Recieved Packets}}{\sum \text{Send Packets}} \times 100 \qquad (۲)$$

به عبارتی نسبت بسته‌های اطلاعاتی دریافت شده بر تعداد بسته‌های ارسال شده در شبکه بر حسب درصد است. مسلماً هرچقدر این میزان درصد بالاتر باشد برآیند راندمان شبکه بهتر است (شکل ۴).

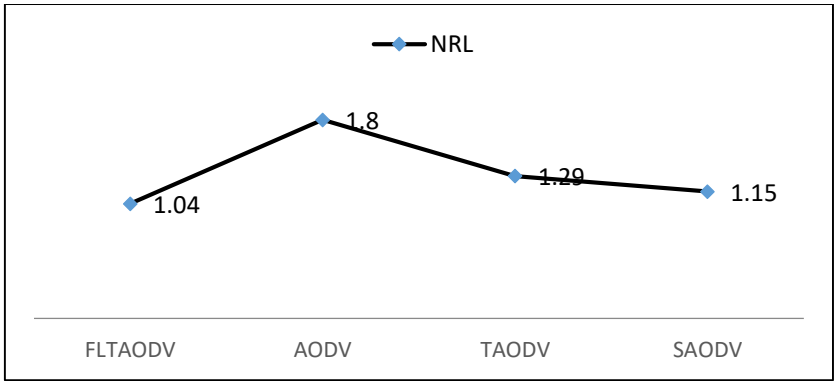


شکل ۴: نمودار نرخ تحویل بسته‌های مسیریابی در زمان ۱۰۰۰ ثانیه

۴-۴ آزمون بار مسیریابی نرمال

یک پارامتر دیگر که در ارزیابی نتایج شبیه‌سازی بررسی کرده‌ایم پارامتر بار نرمال مسیریابی است. هر چه مقدار این پارامتر کمتر باشد نشان دهنده‌ی بارگذاری سریعتر پروتکل مسیریابی هست. نتایج شبیه‌سازی نشان می‌دهد (شکل ۵) پروتکل پیشنهادی به میزان دو برابر از پروتکل پایه سریعتر بارگذاری شده و مسیریابی را سریعتر انجام می‌دهد. این پارامتر نیز جزء موارد مهم و تاثیرگذار در امر مسیریابی شبکه بوده و مطابق فرمول زیر قابل محاسبه است:

$$\text{NRL} = \frac{\sum \text{Send Packets} + \sum \text{Forward Packets}}{\sum \text{Receive Packets}} \times 100 \qquad (۳)$$



شکل ۵: تعداد میزان بار بسته های مسیریابی در زمان ۱۰۰۰ ثانیه

به عبارتی نسبت مجموع بسته‌های اطلاعاتی ارسال شده و جلورانده شده بر تعداد بسته‌های اطلاعاتی دریافت شده در شبکه است که بر حسب درصد محاسبه می‌گردد. مسلماً هرچقدر این میزان درصد پایین‌تر باشد راندمان بهتر شبکه است.

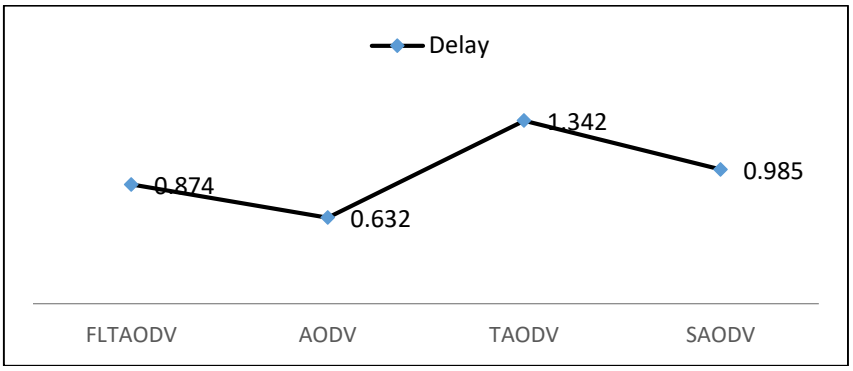
۴-۵ آزمون تاخیر انتها به انتهای شبکه

در این رابطه میزان میانگین تاخیر انتها به انتهای شبکه هدف است. لذا مجموع مدت زمان تفاوت بین زمان ارسال بسته و تحویل آن در مقصد را بر روی تعداد بسته‌های عبوری می‌نماییم. (شکل ۶) به‌عنوان‌مثال زمان ارسال بسته را Ts و زمان دریافت آن بسته را Tr می‌نامیم. به ازای هر بسته عبوری در شبکه یک کانکشن ایجاد می‌شود. لذا برای محاسبه مدت زمان تاخیر شبکه را از رابطه زیر محاسبه می‌کنیم.

$$\text{Average End to End Delay} = \frac{\sum (\text{Tr} - \text{Ts})}{\sum \text{Numberof Connections}} \qquad (۴)$$

تعریف عمومی تاخیر انتها به انتها را به شکل زیر ارایه داده‌ایم.

$$\text{Average End to End Delay} = \frac{\sum(\text{Arrive Time} - \text{Send Time})}{\sum \text{Numberof Connections}} \quad (۵)$$

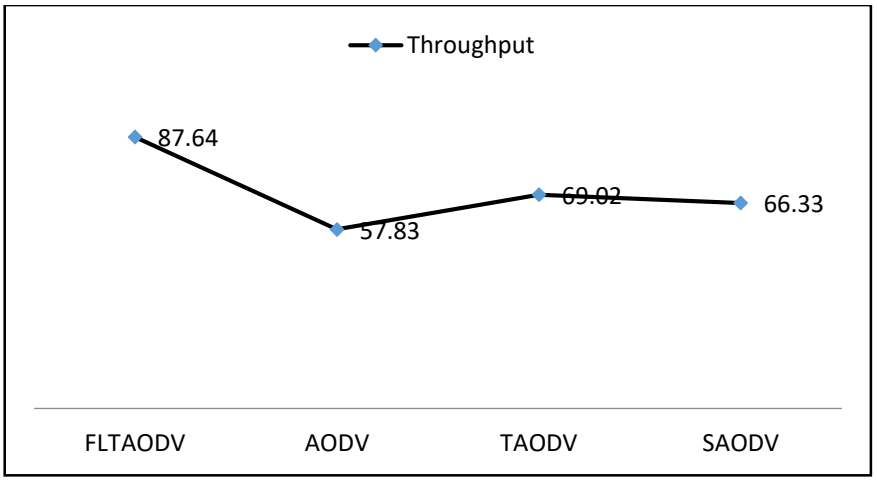


شکل ۶: نمودار تاخیر در مدت زمان ۱۰۰۰ در پروتکل مسریابی

۶-۴ آزمون توان عملیاتی شبکه

این پارامتر میزان راندمان شبکه را در ازای بسته‌های در جریان شبکه و میانگین زمان این جریان بررسی می‌نماید(شکل ۷):

$$\text{hroughput } \mathbf{Packets} = \frac{\text{Flow Number}}{\text{Duration Total}} \quad (۶)$$

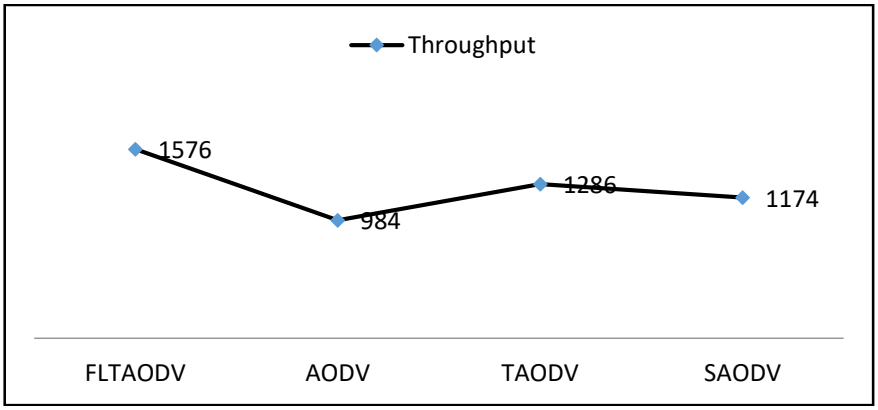


شکل ۷: گذردهی بر اساس بسته های جاری

روش دیگر محاسبه توان عملیاتی شبکه بر اساس تعداد بیت انتقالی شبکه بر زمان جریان می باشد (شکل ۸) که طبق رابطه زیر تعریف می‌شود:

$$\text{Throughput Bits} = \frac{\text{Bit Total}}{\text{Duration Total}} \quad (۷)$$

در این رابطه توان عملیاتی بسته‌ها برابر با حاصل تقسیم تعداد جریان داده بر مدت زمان جریان می‌باشد. هر چقدر این میزان بالاتر با شد ن شانگر راندمان بهتر شبکه ا ست بعبارتی جریان داده بی شتر در واحد زمان فعال ا ست. رابطه دیگر توان عملیاتی مقدار داده بر حسب بیت است. این مقدار نیز هرچقدر بالاتر باشد نمایانگر راندمان بهتر شبکه است.



شکل ۸: توان عملیاتی شبکه بر اساس تعداد بیت انتقالی شبکه

۷-۴ نتیجه گیری

در این تحقیق یک پروتکل مسیریابی مبتنی بر اعتبار و اعتماد با بهره گیری از منطق فازی ارایه شد. درروش پیشنهادی ابتدا میزان اعتبار یک گره همسایه در شبکه توسط همسایگان سنجیده می شود، که این برآیند تابع فازی پیشنهادی است. بر اساس تابع فازی و بدلیل رویدادهای مختلفی که ممکن است در شبکه پیش آید صرفاً به اعتبار و اعتماد دور جاری بسنده نکرده این و به عبارتی از گذشته خوب یا بد یک گره برای محاسبه اعتماد آتی گره استفاده کرده ایم. درصد خطای پایین روش پیشنهادی در تعیین میزان اعتماد یک گره در شبکه نکته بارز این تحقیق است که توانسته است پس از بروز حمله گره‌های مخرب را تشخیص داده و با قرنطینه سازی آن‌ها از ادامه فعالیت آن‌ها جلوگیری کند. نتایج شبیه سازی نشان داده است که روش پیشنهادی تقریباً در تمامی آزمون-های موثر توانسته است نسبت به سایر روش های مشابه بهبود داشته باشد.

مراجع

[1] Zahariadis, Theodore, Helen C. Leligou, Panagiotis Trakadas, and Stamatis Voliotis. "Trust management in wireless sensor networks." European Transactions on Telecommunications 21, no. 4 (2010): 386-395.

[۲] خدیجه نخعی "به کار گیری الگوریتم تطبیقی برای تعیین اعتماد بین گره‌های شبکه حسگر "پایان‌نامه کارشناسی ارشد ،دانشگده مهندسی فناوری اطلاعات گرایش مخابرات امن ،دانشگاه علم و صنعت ،خردادماه ۱۳۸۹

[3] Zahariadis, Theodore, Helen C. Leligou, Panagiotis Trakadas, and Stamatis Voliotis. "Trust management in wireless sensor networks." European Transactions on Telecommunications 21, no.

[4] Zhan, G., Shi, W., Deng, J. (2012) Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING. VOL. 9, NO. 2.

[5] Zahariadis, T., Leligou, H., Karkazis, P., Trakadas, P., Papaefstathiou, I., Vangelatos C., Besson, L. (2010) DESIGN AND IMPLEMENTATION OF ATRUST-AWARE ROUTING ROTOCOL FOR LARGEWSNS. International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3

[6] AsadPirzada, A., McDonald, C. (2007) Trusted Greedy Perimeter Stateless Routing. IEEE ICON.

[7] P.Samundiswary, “Trust based Energy aware Reactive Routing Protocol for Wireless Sensor Networks”, International Journal of Computer Applications (0975 – 8887) Volume 43– No.21, April 2012

[8] Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis,Panagiotis Trakadas, Ioannis Papaefstathiou,Charalambos Vangelatos, Lionel Besson, "DESIGN AND Implementation of

atrust-aware routing protocol for large wsns", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010

[9] Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. Journal of Network and Computer Applications, 35(3), 867-880.

[10] Dogan, G., & Brown, T. (2014). A Survey of Provenance Leveraged Trust in Wireless Sensor Networks. Computer Engineering and Intelligent Systems, 5(2), 1-11.

[11] Bao, F., Chen, R., Chang, M., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. Network and Service Management, IEEE Transactions on, 9(2), 169-183.

[12] Devisri, S., & Balasubramaniam, C. (2013). Secure routing using trust based mechanism in wireless sensor networks (WSNs). International Journal of Scientific & Engineering Research, 4(2), 1-7.

[13] Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 80(3), 602-617.

Trust-based routing in wireless sensor networks using fuzzy logic

H. Moemenzadeh Haghighi[1], Fatemeh Bavi[1], Masoud Etesami[2]

[1]Islamic Azad University, Bushehr branch, Bushehr, Iran

[2]Islamic Azad University, Genaveh branch, Bushehr, Iran

Adstract

Wireless sensor networks, network generation with high potential in the field of the most unpredictable and dynamic environments. However, this network because of its open media, changing and dynamic topology and routing algorithms is fragile. Ad hoc networks and wireless networks support different features, such as dynamic self-organizing, self-configuring, self-correction, high scalability, easy maintenance and reliable services, despite its many features already mentioned, this network is very susceptible to damage from attacks. The absence of a central control system known weakness is perhaps the most important reason. Hierarchical dynamic network topology also allows the implementation of security mechanisms disclaims grid design. By reliable way to offer solutions that can change the nature of attacks against network node that is a dangerous counter attack in this area and to restore network. Characteristic features of the method, computational overhead and minimal power dissipation on the one hand and preventing attacks on the network works. Strategy and the proposed mechanism is evaluated using the simulator NS2.

Keywords: Criteria confidence, trust-based protocols, sensor networks