

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

استادیار، دانشگاه آزاد اسلامی، واحد بوشهر، گروه برق بوشهر، ایران، Momenzadeh.hossein@gmail.com

کارشناس ارشد، دانشگاه آزاد اسلامی، واحد بوشهر، گروه کامپیوتر بوشهر، ایران، Fatemehbavi@yahoo.com

کارشناس ارشد، دانشگاه آزاد واحد گناوه، گروه ریاضی گناوه، ایران Etesami.masoud@yahoo.com

تاریخ دریافت: ۹۵/۱۱/۱۸ تاریخ پذیرش: ۹۶/۲/۱۲

چکیده

شبکه های حسگر بی سیم، حوزه ی پرکاربردی از نسل های شبکه با پتانسیل بالا در محیط های غیرقابل پیش بینی و پویا است. با این حال، این شبکه ها به دلیل رسانه ی باز خود، توپولوژی در حال تغییر و پویا و الگوریتم های مسیریابی آن آسیب پذیر است. شبکه های موردی و شبکه های بی سیم ویژگی های مختلف مثل خود سازمان دهی پویا، خود پیکربندی، خود تصحیحی، نگهداری آسان، مقیاس پذیری بالا و سرویس های مطمئن را پشتیبانی می کند. علیرغم ویژگی های 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 مکانیسم های سلسله مراتبی امنیتی را از طراحان شبکه سلب می نماید. توسط راهکار های مبتنی بر اعتماد روشی پیشنهاد داده می شود که بتواند در برابر حملات تغییر ماهیت گره شبکه که به نوعی خطرناکترین حمله نیز در این حوزه محسوب می شود، مقابله و شبکه را بازیابی کند. از ویژگی های بارز این روش، سربرار محاسباتی و اتلاف انرژی ناچیز از یک سو و مقابله و ترمیم آثار حملات صورت گرفته در شبکه است. راهکار و مکانیسم پیشنهادی با استفاده از نرم افزار شبیه ساز NS2 مورد ارزیابی قرار گرفته 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 گره های مخرب را تشخیص داده و با قرنطینه سازی آن ها از ادامه فعالیت آن ها جلوگیری کند.

کلید واژه: معیارهای اعتماد، پروتکل مبتنی بر اعتماد، شبکه های حسگر

۱- مقدمه

و شیوه های انتقال و تبادل اطلاعات بین گره های شبکه است که وابستگی شدیدی به محدودیت ها، منابع موجود و امکانات فراهم شده از لایه های 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 ارائه شده است، [10,11,12,13] اما پیش از انجام فرآیند مسیریابی در شبکه های حسگر موضوع مهم ایجاد یک مسیر امن جهت ردوبدل شدن داده ها احساس شده است. یکی از ابزارهای مورد استفاده برای ایجاد یک مسیریابی امن در شبکه های حسگر مکانیسم اعتماد است و ما در این مقاله از آن استفاده خواهیم کرد. مدل های اعتماد و اعتبار ابزار مهمی هستند که در بسیاری از زمینه ها مانند اجتماعی، اقتصادی و علوم کامپیوتر مورد استفاده قرار می گیرند.

تکنیک ها و شیوه های مورد استفاده در شبکه های حسگر، وابستگی شدیدی به ماهیت کاربرد، ساختار توپولوژی شبکه، شرایط جوی و محیطی، محدودیت ها و پارامترهای کارایی و هزینه دارند. لذا امروزه در سرتاسر دانشگاه های معتبر و مراکز تحقیقاتی کامپیوتری، الکترونیکی و مخابراتی، شبکه های حسگر بی سیم یک فیلد تحقیقاتی بسیار جذاب و پرطرفدار محسوب می شود.

هدف اصلی تمامی این تلاش ها و ارائه راهکارها، داشتن سیستمی با شیوه های کنترلی ساده، آسان و با هزینه پایین هست که در نهایت با پاسخگویی به نیازمندی های مدنظر بتواند در مقابل محدودیت ها (پهنای باند، انرژی، دخالت های محیطی و ...) ایستادگی کند و شرایط کلی را طبق خواسته ها و تمایلات موجود (انتقال حجم زیاد اطلاعات پرمحتوا، بقاء پذیری، امنیت و طول عمر بالا، هزینه پائین و ...) فراهم سازد. از مباحث موجود و مهم در شبکه های حسگر، بحث مسیریابی

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 می‌شود. 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 کنترل انرژی سطح انرژی ها را به روز می‌کند و در صورت تحویل گره عدد، ۱ و در غیر این صورت صفر ذخیره می‌شود. 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 رخدادهای اتفاق افتادند، سطح اعتماد آن گره به روز می‌شود [۵]. در [۴] یک پروتکل مسیریابی برای اجتناب از مکان‌های ناامن ارائه شده است. این

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 به صورت موقتی شکل می‌گیرند و توسط خود گره‌ها سازمان‌دهی می‌شوند گره‌های بدخواه به خوبی تغییر شکل می‌دهند و می‌توانند با استفاده از خصوصیت ذاتی مشارکت گره‌ها در فرآیندهای شبکه حسگر به عناصر شبکه حمله کنند. به عنوان مثال تهدیدات امنیتی مانند استراق سمع، کرم‌چاله، رفتار نوسانی و سیاه‌چاله و... در شبکه‌های حسگر از این دسته هستند که به طور ویژه، فرآیندهای مسیریابی را هدف قرار می‌دهند. وجود چنین خصوصیتی 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، بااین حال 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. از این رو می‌توان گفت که برای داشتن کاربردهای امن و قابل اطمینان در شبکه‌های حسگر، مدیریت اعتماد نیازمند هست [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 مبدأ، 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 از یک سیستم تبادل شهرت پیچیده استفاده می‌کند. هسته شهرت

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 است. برای اینکه این فرآیند تشخیص داده شود و به‌موقع با آن برخورد شود از یک مکانیسم اعتماد چند سطحی استفاده شده است. در روش 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 پیشنهادی حاصل می‌شود که خود تاثیر پذیر از سه پارامتر دیگر است که این سه پارامتر شامل: نسبت سوئیچ کردن گره، میزان تأخیر انتها به انتهای مسیری که گره مذکور در آن شرکت داشته و اختلاف زمانی اکنون و زمان آخرین تراکنش گره است. در مرحله بعد این میزان اعتماد به‌عنوان اعتماد گذشته شناخته می‌شود. دلیل استفاده 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 داشته‌اند نشان می‌دهد که این سه ویژگی را نداشته است. اما به جز سه پارامتر فوق، 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 گرفته شده است تا هم اعتماد در روش کلی دخالت داده شود و هم اعتبار یک مسیر، 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 بایست از لحاظ 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. هر قدر این تأخیر بالاتر باشد نشان‌دهنده شلوغ بودن مسیر است و مدت‌زمان قرارگیری بسته‌ها در صف گره‌های واسط بالاست. [7]

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 [6] 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 در نظر گرفته می‌شود. با توجه به قابلیت‌های پروتکل پایه، بسته جدیدی تولید نمی‌شود. بلکه با استفاده از ساختار موجود، روش‌ها و فرمول‌های آماری را در نظر گرفته می‌شود که با استفاده از آن‌ها و برخی پارامترهای موجود در جداول مسیریابی سعی در تخمین میزان اعتماد به هر گره و مسیر را داریم. 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 می‌باشد) از 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 به گونه‌ای 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 طول عمر شبکه حسگر را تا حد ممکن افزایش دهد.

۲- روش اعتماد پیشنهاد شده

در روش پیشنهادی هدف تشخیص و مقابله با گره‌ای است که مدام بین رفتار خوب و بد سوئیچ می‌کند. در حالت خوب همانند سایر گره‌های

جدول ۳-۱: 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

با توجه به معادله زیر پس از جاگذاری، شرایط عددی زیر می باشد :
 رابطه (۱)

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

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

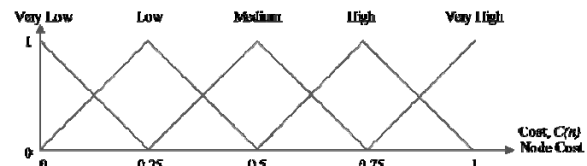
میزان اعتماد گره با توجه به ورودی های ما برای این گره برابر 0.346 است .

۴- شبیه سازی، ارزیابی و مقایسه روش پیشنهادی

در مسیریابی مبتنی بر اعتماد، چندین حالت مختلف را می توان در نظر گرفت. اعتماد گره به گره، اعتماد گره به لینک و بالعکس از مواردی بوده که در شبکه های بی سیم قابل پیاده سازی است. ضمناً هرکدام از این روش ها می تواند بطور غیر مستقیم نیز پیاده سازی شود بطوری که یک گره از طریق رخدادهای شبکه و دریافت گزارشات همسایگان میزان اعتماد خود به گره همسایه را پیش بینی و ارزیابی نماید. از این رو راه حل های گوناگونی را می توان جهت پیاده سازی مکانیسم اعتماد شبکه در نظر گرفت. که در روش پیشنهادی به صورت ترکیبی از منطق فازی جهت تخمین و اعطای درجه اعتماد گره های شبکه، استفاده شده است . اما همواره ترکیبی از اعتبار (منظور از اعتبار همان کیفیت لینکی است که شامل تعدادی گره معتمد است). یعنی معیار اعتماد نهایی وابسته به پارامترهای مسیریابی شامل تاخیر و میزان دسترسی به گره

اختلاف زمانی اکنون و زمان آخرین تراکنش گره یک بازه زمانی است. از ۱۰ ثانیه استفاده شده است . این نمونه برداری نباید خیلی کوتاه باشد تا دچار تغییرات لحظه ای شبکه نشود و نه خیلی طولانی که نتایج کلی به نظر آیند. لذا این زمان نمونه برداری را به دلخواه و با توجه به نیاز شبکه متغیر در نظر گرفته می شود. در خصوص زمان شبیه سازی نیز چون از شبیه ساز NS2 استفاده شده است و NS2 از گونه شبیه سازهای رویدادگردان است و از طریق پیگیری رخدادهای در طول زمان های گسسته، شبیه سازی را پیش میبرد. این شبیه ساز در دو محیط برنامه نویسی ++C و OTCL و به صورت شیء گرا طرح شده است. ورودی های ما سه عنصر تعداد سوئیچ، تاخیر و اختلاف زمان می باشد.

همان طور که از منطق فازی و مدل مثلثی برمی آید، هر پارامتر ورودی سیستم فازی شامل یک نمودار مثلث بندی است. در هر نمودار با توجه به مثلث های مشخص و یکسان می توان 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. (شکل ۳-۱)



شکل ۳-۱: نمودار تعداد سوئیچ کردن های گره به حالت خوب و بد

و اگر گره ما دارای switch = 0.6

Delay=0.3

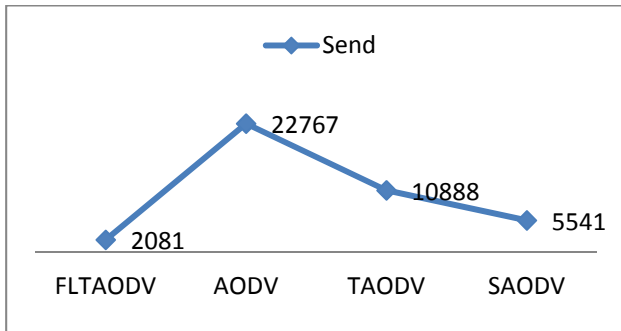
Time Defrence=5.2

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 عبارتند از (جدول ۳-۱):

کاهش خواهد یافت. (شکل ۴-۲)



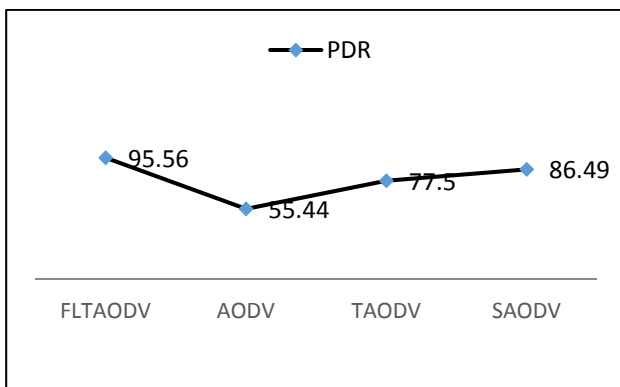
شکل ۴-۲: نمودار تعداد بسته های مسیریابی از دست رفته در زمان ۱۰۰۰ ثانیه: با استفاده از اعتماد سه سطحی و انتخاب بسته های با اعتماد بالاتر حداقل از دست دادن بسته را داراست.

۴-۳: آزمون نرخ تحویل بسته ها

این مقدار بر حسب درصد و بر اساس فرمول زیر محاسبه می گردد: رابطه (۲)

$$PDR = \frac{\sum Recieved\ Packets}{\sum Send\ Packets} \times 100$$

به عبارتی نسبت بسته های اطلاعاتی دریافت شده بر تعداد بسته های ارسال شده در شبکه بر حسب درصد است. مسلماً هرچقدر این میزان درصد بالاتر باشد برآیند راندمان شبکه بهتر است. (شکل ۴-۳)

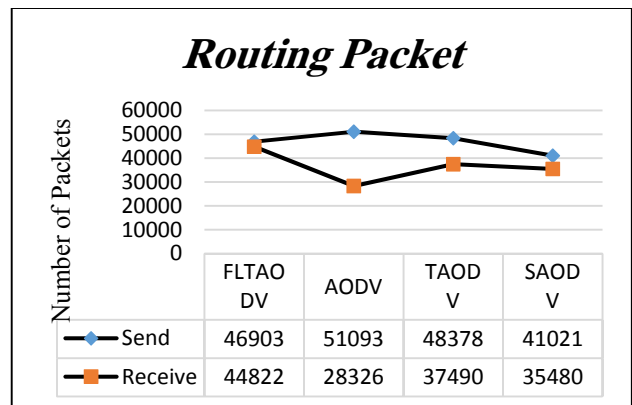


شکل ۴-۳: نمودار نرخ تحویل بسته های مسیریابی در زمان ۱۰۰۰ ثانیه: پروتکل تغییر یافته جدید نسبت به بقیه بهتر عمل می کند بدلیل اینکه مسیرهای بهتری مشخص شده و بسته های کمتری از دست رفته است و استفاده از مسیرهای نامعتبر سبب می شود نرخ تحویل بسته ها رضایت بخش نباشد.

می باشد. بنابر این این گره و گره های بعدی در لینک ایجاد شده دارای اعتبار است. و اعتماد در شبکه می تواند مفید باشد. زیرا اگر تصمیم مناسبی در خصوص همسایه نامعتبر یا نامعتبر وجود داشته باشد شبکه ممکن است به شکست لینک یا ارتباطات ناحیه ای منجر شود. در این مقاله شبیه سازی بر روی پروتکل مسیریابی پایه AODV قرارداد شده است. این شبیه سازی در محیط NS2.34 پیاده سازی شده و نتایج شبیه سازی در ادامه این فصل به ترتیب نوع آزمون آورده شده است. (در تمامی شکل ها پروتکل پیشنهادی FLTAODV نامیده ام)

۴-۱: آزمون تعداد بسته های مسیریابی

این پارامتر جهت ارزیابی پروتکل پیشنهادی با پروتکل های همردیف خود در نرخ مسیریابی بسته های شبکه انجام شده است. آزمون مذکور نشان دهنده تعداد بسته های ارسالی و دریافتی بوده تا بتوان از این ارزیابی به این نتیجه رسید که پروتکل تا چه حد توانسته است بسته های تولید شده در شبکه را سالم به مقصد تحویل دهد. معمولاً هر چقدر فاصله تعداد بسته های ارسالی و دریافتی به یکدیگر نزدیک تر باشد روند پروتکل مناسب تر خواهد بود. (شکل ۴-۱)



شکل ۴-۱: نمودار تعداد بسته های مسیریابی در زمان ۱۰۰۰ ثانیه:

{ 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. }

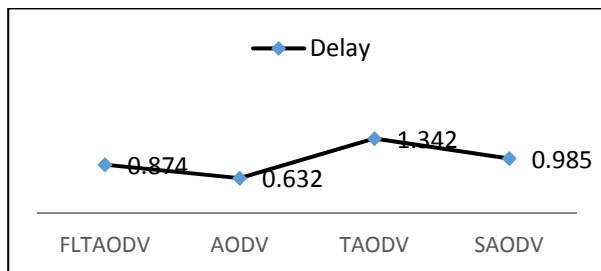
۴-۲: آزمون تعداد بسته های از دست رفته

در مسیریابی شبکه هر قدر فرآیند مسیریابی در انتقال بسته های اطلاعاتی موفق عمل کند تعداد بسته های از دست رفته در شبیه سازی

مسیریابی مبتنی بر اعتماد در شبکه های حسگر بی سیم با ...

تعریف عمومی تاخیر انتها به انتها به شکل زیر ارائه می شود .
 رابطه (۵)

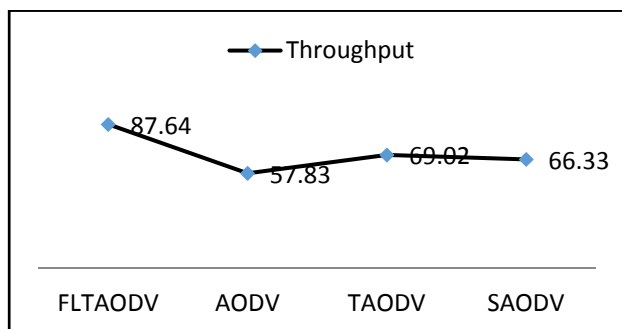
$$\text{Average End to End Delay} = \frac{\sum (\text{Arrive Time} - \text{Send Time})}{\sum \text{Number of Connections}}$$



شکل ۴-۵: نمودار تاخیر در مدت زمان ۱۰۰۰ در پروتکل مسیریابی: نگهداری مداوم مسیر منجر به افزایش تعداد مسیرهای جایگزین معتبر می شود. از این رو زمان میان از بین رفتن مسیر اصلی و بدست آوردن یک مسیر جدید افزایش پیدا می کند.

۴-۶: آزمون توان عملیاتی شبکه این پارامتر میزان راندمان شبکه را در ازای بسته های در جریان شبکه و میانگین زمان این جریان بررسی می نماید (شکل ۴-۶):
 رابطه (۶)

$$\text{Throughput Packets} = \frac{\text{Flow Number}}{\text{Duration Total}}$$



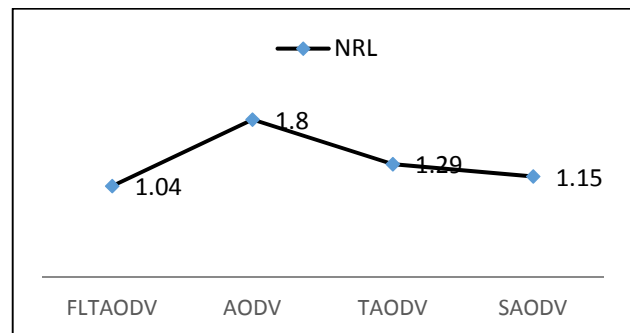
شکل ۴-۶: گذردهی بر اساس بسته های جاری: هنگامیکه یک مسیر دچار ازدحام شود، ارسال کننده سعی در ایجاد ارتباط جدید و ارسال مجدد از طریق مسیر جدیدی مینماید. این عمل سربار، صرف زمان، انرژی و پردازش بیشتری را در پی خواهد داشت. که در پروتکل پیشنهادی بدلیل استاده از مسیرهای کوتاهتر و استفاده از اعتماد سه

۴-۴: آزمون بار مسیریابی نرمال

یک پارامتر دیگر که در ارزیابی نتایج شبیه سازی بررسی شده است پارامتر بار نرمال مسیریابی است. هر چه مقدار این پارامتر کمتر باشد نشان دهنده ی بارگذاری سریعتر پروتکل مسیریابی هست. نتایج شبیه سازی نشان می دهد (شکل ۴-۴) پروتکل پیشنهادی به میزان دو برابر از پروتکل پایه سریعتر بارگذاری شده و مسیریابی را سریعتر انجام می دهد. این پارامتر نیز جزء موارد مهم و تاثیرگذار در امر مسیریابی شبکه بوده و مطابق فرمول زیر قابل محاسبه است:

رابطه (۳)

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



شکل ۴-۴: تعداد میزان بار بسته های مسیریابی در زمان ۱۰۰۰ ثانیه {به عبارتی نسبت مجموع بسته های اطلاعاتی ارسال شده و جلورانده شده بر تعداد بسته های اطلاعاتی دریافت شده در شبکه است که بر حسب درصد محاسبه می گردد. مسلماً هر چقدر این میزان درصد پایین تر باشد نتیجه 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 تعداد بسته های عبوری نامیده می شود. (شکل ۴-۵) به عنوان مثال زمان ارسال بسته Ts و زمان دریافت آن بسته Tr می باشد. به ازای هر بسته عبوری در شبکه یک کانکشن ایجاد می شود. لذا برای محاسبه، مدت زمان تاخیر شبکه از رابطه زیر محاسبه می شود.
 رابطه (۴)

$$\text{Average End to End Delay} = \frac{\sum (Tr - Ts)}{\sum \text{Number of Connections}}$$

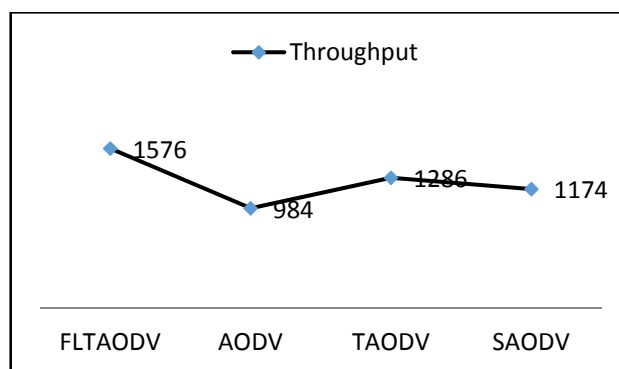
سطحی گذردهی بهتری را مشاهده می کنیم .

روش دیگر محاسبه توان عملیاتی شبکه بر اساس تعداد بیت انتقالی شبکه بر زمان جریان می باشد (شکل ۴-۷) که طبق رابطه زیر تعریف می شود:

رابطه (۷)

$$\text{Throughput Bits} = \frac{\text{Bit Total}}{\text{Duration Total}}$$

در این رابطه توان عملیاتی بسته‌ها برابر با حاصل تقسیم تعداد جریان داده بر مدت زمان جریان می‌باشد. هر چقدر این میزان بالاتر باشد نشانگر راندمان بهتر شبکه است عبارتی جریان داده بیشتر در واحد زمان فعال است. رابطه دیگر توان عملیاتی مقدار داده بر حسب بیت است. این مقدار نیز هرچقدر بالاتر باشد نمایانگر راندمان بهتر شبکه است.



۵ - نتیجه گیری :

در این تحقیق یک پروتکل مسیریابی مبتنی بر اعتبار و اعتماد با بهره گیری از منطق فازی ارائه شد. در روش 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 شده است . 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 آزمون‌های موثر توانسته است نسبت

به سایر روش های مشابه بهبود داشته باشد.

در جدول ۵-۱ ، پارامترهایی که در شبیه‌سازی راهکار پیشنهادی مدنظر قرار گرفت آورده شده است.

جدول ۵-۱ : شرایط شبیه سازی پیشنهادی

پروتکل	FLTAODV	AODV	TAODV	SAODV
پارامتر	802.11	802.11	802.11	802.11
پروتکل MAC	802.11	802.11	802.11	802.11
پروتکل مسیریابی	Trust and Reliability	AODV	TAODV	SAODV
تعداد گره	۳۰	۳۰	۳۰	۳۰
توزیع گره‌ها	تصادفی	تصادفی	تصادفی	تصادفی
تعداد گره مخرب	ثابت و تصادفی	ثابت و تصادفی	ثابت و تصادفی	ثابت و تصادفی
برد رادیویی گره	۲۵۰ متر	۲۵۰ متر	۲۵۰ متر	۲۵۰ متر
محیط شبیه‌سازی	۱۰۰۰ متر	۱۰۰۰ متر	۱۰۰۰ متر	۱۰۰۰ متر
لایه فیزیکی	Phy Wireless	Phy Wireless	Phy Wireless	Phy Wireless
نوع آنتن	همه جهته	همه جهته	همه جهته	همه جهته
نوع صف	Drop Tail/PreQ	Drop Tail/PreQ	Drop Tail/PreQ	Drop Tail/PreQ
زمان شبیه‌سازی	۱۰۰۰ ثانیه	۱۰۰۰ ثانیه	۱۰۰۰ ثانیه	۱۰۰۰ ثانیه

با توجه به جدول شماره ۵-۲ ، نتایج حاکی از آن است که پروتکل پیشنهادی در پارامترهای موثر شبکه از جمله نرخ بسته‌های از دست رفته، نرخ مسیریابی نرمال، نرخ تحویل بسته‌های اطلاعاتی شبکه و

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.

میانگین نرخ گذردهی شبکه بسیار بهتر از پروتکل های همردیف عمل نموده و راندمان بهتری داشته است.

throughput	DELAY	NRL	PD R	DR OP	SEND RESERVE	پروتکل
87.64	0.874	1.04	95.56	2081	4690344822	FLTA ODV
57.83	0.632	1.8	55.44	22767	5109328326	AODV
69.02	1.342	1.29	77.5	10888	4837837490	TAODV
66.33	0.985	1.15	86.49	5541	4102135480	SAODV

جدول ۵-۲ نتایج شبیه سازی

با توجه به مطالب بیان شده در این پایان نامه، در مباحث مختلف شبکه های حسگر می توان از روش اعتماد به منظور تامین و حفظ امنیت پروتکل های فعال مسیریابی استفاده نمود و از اطلاعات توپولوژیکی ذاتی این قبیل پروتکل ها بطور مستقیم و یا غیر مستقیم مکانیسم اعتماد را پیاده سازی نمود. در این بخش ما از معیار اعتماد مستقیم و غیر مستقیم به صورت ترکیبی بهره جسته ایم اما این قبیل پروتکل ها قابلیت پیاده سازی اعتمادهایی از قبیل گره به گره، گره به لینک و لینک به چاهک و بلعکس را دارد، و پژوهشگران میتوانند در آینده بر روی این مباحث پیاده سازی داشته باشند.

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 گره های شبکه حسگر" پایان نامه کارشناسی ارشد، دانشگاه 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 (2010): 386-395.
- [4] Zhan, G., Shi, W., Deng, J. (2012) Design and Implementation of TARS: A Trust-Aware Routing Framework for WSNs. *IEEE*