



مدیریت اعتماد توزیع شده و مقیاس پذیر در شبکه های حسگر

بی سیم

خدیدجه نخعی^۱، هادی شهریار شاه حسینی^۲
دانشگاه علم و صنعت ایران، دانشکده برق^۱

hshsh@iust.ac.ir

چکیده

راه حل های امنیتی که برای شبکه های حسگر پیشنهاد شده اند اغلب با فرض وجود یک محیط قابل اعتماد به وجود آمده اند، در حالی که معمولاً این گونه نیست. بنابراین مدیریت اعتماد نیاز اساسی ارائه راه حل های امنیتی در شبکه هاست. طرح های مدیریت اعتماد موجود که برای سایر شبکه ها طراحی شده اند، برای شبکه های حسگر مناسب نیستند زیرا مقدار زیادی انرژی و حافظه مصرف می کنند. از سوی دیگر شبکه های حسگر معمولاً دارای تعداد زیادی گره می باشند و این مسئله باعث می شود مقیاس پذیری مدل اعتماد از اهمیت خاصی برخوردار باشد. در این مقاله مدل اعتماد توزیع شده ای برای شبکه های حسگر بیسیم پیشنهاد می شود که در آن هر گره از دو منبع اعتماد مستقیم و غیرمستقیم برای محاسبه اعتماد استفاده می کند و از طرف دیگر هر گره تنها اعتماد گره های همسایه خود را نگه می دارد، از این رو به ساختار کلی شبکه و تعداد گره های آن وابسته نیست و بنابراین مقیاس پذیر است. شبیه سازی ها نشان می دهند که مدل اعتماد پیشنهادی صرف نظر از تعداد گره های شبکه رفتار مشابهی در کلیه آن ها دارد و اگر تعداد کارپذیرهای بدخواه کمتر از ۵۰٪ کل کارپذیرها باشد، میزان دستیابی کارخواه ها به کارپذیرهای قابل اعتماد در شبکه های با تعداد مختلف گره حسگر بیشتر از ۹۰٪ است.

واژه های کلیدی

مدل اعتماد، اعتماد مستقیم، اعتماد غیرمستقیم، شبکه حسگر بی سیم.

۱- مقدمه

شبکه حمله کنند. همچنین این خصوصیت شبکه های حسگر بیسیم که مستعد خطا می باشند، باعث ناپایداری این شبکه ها می گردد. بنابراین چگونگی انتخاب گره های همکار در تراکنش ها برای افزایش بازده اهمیت زیادی پیدا می کند [۲]. مدل های اعتماد ابزار مناسبی برای دستیابی به این هدف می باشند.

مفهوم مدیریت اعتماد، که اعتماد را در اجزای شبکه مدل می کند، می تواند برای این شبکه ها مفید باشد. اعتماد علاوه بر آن که می تواند در مورد خودسازمان دهی گره های شبکه در برابر تغییرات رخ داده در همسایگی آن ها کمک کند، می تواند در برقراری پروتکل های امنیتی نیز شرکت کند. یک سامانه مدیریت اعتماد می تواند برای آشکارسازی گره هایی که به درستی رفتار نمی کنند نیز مفید باشد، و یا می تواند در تصمیم گیری به گره ها کمک کند [۳].

شبکه های حسگر بی سیم شبکه هایی براساس همکاری گره های کوچک می باشند. این گره ها اساساً با مصرف انرژی کم، هزینه اندک و ارتباطات بیسیم مشخص می شوند. آن ها می توانند برای اندازه گیری دما، فشار، رطوبت، نور و ... به کار روند، اما دارای محدودیت هایی مانند محدودیت حافظه، قدرت محاسباتی و انرژی هستند [۱]. این شبکه ها با توجه به کاربرد آن ها دارای تعداد مختلف گره حسگر می باشند.

شبکه های حسگر به صورت موقتی شکل می گیرند و توسط خود گره ها سازماندهی می شوند. در یک شبکه حسگر پیچیده، گره های بدخواه به خوبی تغییر شکل می دهند و می توانند با استفاده از خصوصیت ذاتی مشارکت شبکه های حسگر به عناصر

ATSN [۸] مدلی است که گره های حسگر اعتماد دیگر گره های شبکه را نگه می دارند. یک گره مسئولیت پایش سایر گره ها را به عهده دارد و اعتبار آن ها را به دست می آورد و از این اعتبار برای ارزیابی قابلیت اعتماد و پیش بینی رفتار آینده استفاده می کند. در زمان تراکنش هر گره فقط با گره هایی که به آن ها اعتماد دارد همکاری می کند.

در مدلی که در این مقاله معرفی می شود هر گره مقدار اعتماد گره هایی را که در محدوده رادیویی آن قرار دارند، براساس تراکنش های قبلی و از دو طریق به دست می آورد. این مدل نیاز به یک مرکز اعتماد برای نگهداری مقادیر اعتماد ندارد که به خوبی با شبکه های حسگر بی سیم سازگار است.

۳- فرضیات و توصیف کلی DSTM!

شبکه های حسگر بی سیم با توجه به نوع گره های تشکیل دهنده آن ها دارای انواع مختلفی هستند. در یک دسته بندی، شبکه های حسگر به دو دسته ایستا و پویا تقسیم می شوند، در شبکه های ایستا گره ها مکان مشخصی دارند در حالی که در شبکه های پویا، گره ها به هر جایی حرکت می کنند. در این مقاله شبکه های حسگر به صورت ایستا هستند. برای فراهم کردن شرایط مورد نیاز در شبیه سازی ها فرض می شود برخی از گره ها تقاضاکننده سرویس (یا کارخواه) هستند و برخی دیگر فراهم آورنده سرویس (یا کارپذیر) هستند. همچنین فرض می شود که هر گره فقط همسایه های خود را که در محدوده رادیویی آن هستند می شناسد و هیچ چیز در مورد ساختار کلی شبکه نمی داند.

در مدل اعتماد پیشنهادی (DSTM)، گره ها برای به دست آوردن مقدار اعتماد همسایه های خود از دو منبع اعتماد مستقیم و اعتماد غیرمستقیم استفاده می کنند، هر گره مقادیر اعتماد مستقیم گره هایی که در محدوده رادیویی آن قرار دارند را می داند و علاوه بر آن در مورد هر یک از گره ها از اعتماد غیرمستقیمی که توسط سایر گره ها به دست می آورد استفاده می کند و سپس با ترکیب اعتماد مستقیم و غیرمستقیم یک مقدار اعتماد کلی برای هر گره محاسبه می کند. مقدار اعتماد برای هر گره به صورت عددی در بازه [۰،۱] می باشد.

در ادامه به بیان جزئیات این مدل پرداخته می شود و چگونگی محاسبه اعتماد مستقیم و غیر مستقیم و ترکیب آن ها برای به دست آوردن اعتماد کلی بیان می شود.

با توجه به اهمیت اعتماد در شبکه های حسگر بی سیم از یک سو و از سوی دیگر محدودیت هایی مانند محدودیت انرژی، حافظه و قدرت محاسباتی و تعداد قابل توجه گره حسگر مسأله مهم چگونگی محاسبه اعتماد گره ها مطرح است [۴]. بر این اساس ارائه مدل اعتماد مقیاس پذیر براساس محدودیت های این شبکه ها از اهمیت خاصی برخوردار است.

در این مقاله مدل اعتماد توزیع شده ای معرفی می شود که گره ها برای محاسبه اعتماد یکدیگر از دو منبع آزمایش های مستقیم و غیرمستقیم استفاده می کنند و هر گره فقط مقادیر اعتماد همسایه های خود را نگه می دارد و بیش از این در مورد تعداد گره های تشکیل دهنده شبکه نمی داند. این توزیع شدگی و نحوه محاسبه اعتماد باعث می شود که روش پیشنهاد شده مقیاس پذیر باشد و به این دلیل DSTM^۱ نامیده شده است.

در ادامه این مقاله، در بخش دوم به بررسی اجمالی برخی از مدل های اعتماد موجود برای شبکه های حسگر بی سیم پرداخته می شود، بخش سوم به توصیف کلی مدل اعتماد پیشنهادی (DSTM) اختصاص دارد. در بخش چهارم چگونگی به روز شدن مقادیر اعتماد گره ها مطرح می شود. بخش پنجم شبیه سازی ها را ارائه می دهد و در بخش ششم نیز نتیجه گیری و کارهای آینده بیان خواهد شد.

۲- مروری بر کارهای پیشین!

روش های اعتماد و اعتبار ابزار مهمی هستند که در بسیاری از زمینه ها مانند اجتماعی، اقتصادی و علوم کامپیوتر مورد استفاده قرار می گیرند. سیستم های اعتماد روش مفیدی برای تشخیص تهدیدات اعضای فریبکار یا اعضای در خطر افتاده یک شبکه هستند. این سیستم ها با شناسایی گره های بدخواه و حذف آن ها از شبکه کار خود را انجام می دهند [۵].

RFSN [۶] اولین مدل اعتمادی است که منحصراً برای شبکه های حسگر بی سیم طراحی و گسترده شده است و از روش سگ نگهبان^۲ برای ایجاد اعتماد استفاده می کند. اما سگ نگهبان به خاطر نقایص خودش نمی تواند تمام رفتارها را ثبت کند و بنابراین مقداری نامعینی در این سیستم وجود دارد.

ATRM [۷] یک طرح مدیریت اعتماد برای شبکه های حسگر بی سیم براساس عامل است که مدیریت اعتماد به صورت محلی و با سرباره کمی از نظر پیام و تأخیر اجرا می شود ولی از جمله معایب این مدل این است که یک موجودیت مورد اعتماد مسئول ایجاد و حفظ عامل ها می باشد و همچنین عامل ها در برابر تحلیل های غیرمجاز و اصلاح منطق محاسباتی آن ها آسیب پذیرند.

³ Client

⁴ Server

¹ Distributed & Scalable Trust Model

² Watchdog

۳-۱- اعتماد مستقیم!

در مرحله راه اندازی سامانه مدیریت اعتماد باید برای هر گره مقدار اعتماد اولیه ای در نظر گرفت. اگر مقدار اعتماد اولیه گره ها به یکدیگر زیاد و نزدیک به یک باشد همه گره ها به یکدیگر اعتماد زیادی خواهند داشت و تشخیص گره قابل اعتماد از گره بدخواه مشکل خواهد بود، از طرف دیگر اگر مقدار اولیه اعتماد را مقدار کمی در نظر بگیریم در ابتدا، همه اعضا نسبت به سایرین دچار عدم اعتماد هستند و در این حالت نیز با مشکل قبلی مواجه می شویم [۹]. از این رو مقدار اعتماد مستقیم هر گره برای گره های همسایه اش برابر 0.5 است و در طول تراکنش های مختلف این مقدار اعتماد به روز و به مقدار واقعی نزدیک می شود.

همان طور که قبلاً بیان شد هر گره اعتماد سایر گره ها که در محدوده رادیویی آن قرار دارند را نگه می دارد، از این رو گره ها برای نگهداری مقادیر اعتماد به حافظه کمتری در مقایسه با مدل های اعتماد توزیع شده نیاز دارد [۱۰]. این موضوع با توجه به شکل ۱ مشخص می شود. در این شکل گره ۱ مقدار اعتماد گره های ۲، ۳، ۴ و ۶ را نگه می دارد. مقدار اعتماد مستقیم یک گره به گره دیگر در مرحله n با $T_{i,j}(n)$ که $i, j = 1, 2, 3, \dots$ نشان داده می شود.

۳-۲- اعتماد غیرمستقیم!

برای درک چگونگی محاسبه اعتماد غیرمستقیم، فرض کنید گره i بخواهد اعتماد غیرمستقیم گره j را به دست آورد، بنابراین باید از مقدار اعتماد مستقیمی که سایر گره ها در مورد گره j دارند استفاده کند. ولی تنها گره هایی می توانند به گره i در به دست آوردن اعتماد غیرمستقیم کمک کنند، که گره j در محدوده رادیویی آن ها باشد و از طرف دیگر خود آن گره هم در محدوده رادیویی گره i قرار داشته باشد زیرا در این مدل اعتماد هر گره فقط اعتماد گره های همسایه اش را نگهداری می کند. در شکل ۱ گره های ۳ و ۴ در محدوده رادیویی مشترک گره های ۱ و ۲ قرار دارند، بنابراین گره ۱ برای به دست آوردن اعتماد غیرمستقیم گره ۲ از این دو گره استفاده می کند. اما گره هایی مانند گره ۶ که در محدوده رادیویی گره ۲ نیست و همچنین گره ۵ که در محدوده رادیویی گره ۲ می باشد ولی در محدوده رادیویی گره ۱ قرار نمی گیرد در رابطه اعتماد غیرمستقیم وارد نمی شوند. اعتماد غیرمستقیم گره i به گره j در مرحله n با $R_{i,j}(n)$ نشان داده می شود.

اگر گره i بخواهد مقدار اعتماد غیرمستقیم گره j را به دست آورد، از گره های همسایه اش مقدار اعتماد مستقیم گره j را سؤال می کند و با توجه به اعتمادی که خودش در مورد گره های پاسخ دهنده دارد اعتماد غیرمستقیم گره j را به

صورت زیر محاسبه می کند.

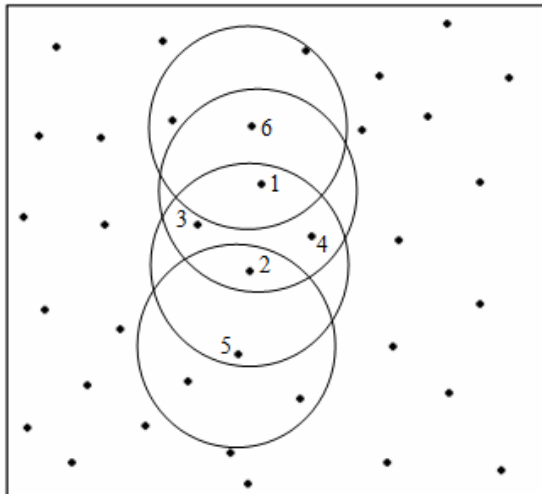
$$R_{i,j}(n) = \frac{1}{N} \sum_k T_{i,k} * T_{k,j}$$

در رابطه (۱)، N تعداد گره های موجود در محدوده مشترک بین گره i و j است و k شماره آن گره ها است. در مثال نمایش داده شده در شکل ۱، اگر $i=1$ و $j=2$ در نظر گرفته شوند، $k=3,4$ است.

۳-۳- اعتماد کلی!

برای محاسبه اعتماد کلی هر گره، اعتماد مستقیم و غیرمستقیمی را که در مراحل قبل به دست آورده با هم ترکیب می کند و یک مقدار اعتماد کلی برای هر یک از همسایگانش به دست می آورد. مقدار اعتماد کلی گره i به گره j با $T'_{i,j}$ نشان داده می شود و از رابطه ۲ به دست می آید.

$$T'_{i,j}(n) = w_1 T_{i,j}(n) + w_2 R_{i,j}(n) \quad (2)$$



شکل ۱: گره ۱ اعتماد مستقیم گره های ۲، ۳، ۴ و ۵ را نگه می دارد. این گره برای به دست آوردن اعتماد غیرمستقیم گره ۲ از گره های ۳ و ۴ کمک می گیرد.

در رابطه (۲)، w_1 و w_2 به ترتیب وزن اعتماد مستقیم و غیرمستقیم هستند و رابطه $w_1 + w_2 = 1$ برقرار است. این دو مقدار با توجه به شرایط محیطی و عملکرد گره ها تغییر می کنند.

۴- به روز کردن مقدار اعتماد!

به روز کردن مقدار اعتماد گره ها به رضایت گره تقاضاکننده از سرویس دریافتی، بستگی دارد. سرویس با یک نام یا شناسه مشخص می شود. اگر گره i سرویسی را درخواست کرده باشد، پس از محاسبه اعتماد گره های همسایه اش به روش بیان شده

دریافت کرده باشد مقدار اعتماد تمامی گره هایی که در رابطه اعتماد غیرمستقیم ظاهر شده اند را به میزان بسیار کمی افزایش می دهد و برعکس اگر کیفیت سرویس دریافتی در حد مطلوب نباشد گره i مقدار اعتماد این گره ها را مقدار بسیار کمی کاهش خواهد داد. کاهش یا افزایش اعتماد گره های سهمی در محاسبه اعتماد غیرمستقیم توسط رابطه ۴ صورت می گیرد.

$$T_{i,k}(n+1) = \begin{cases} T_{i,k}(n) * (1 + \varepsilon) & S_i(n+1) = 1 \\ T_{i,k}(n) * (1 - \varepsilon) & S_i(n+1) = 0 \end{cases} \quad (۴)$$

در رابطه ۴، ε بسیار کوچکتر از β است زیرا نمی توان از روی کیفیت سرویس دریافتی قضاوت کاملی در مورد تمام این گره ها داشت و مقدار اعتماد آن ها نباید تغییر چشمگیری داشته باشد. k گره هایی هستند که در رابطه محاسبه اعتماد غیر مستقیم گره i در مورد j ظاهر می شوند.

۵- شبیه سازی!

برای ارزیابی DSTM از شبیه سازی با نرم افزار TRMSim-WSN استفاده شده است [۱۰]. TRMSim-WSN یک شبیه ساز دامنه آزاد مدل های اعتماد و اعتبار برای شبکه های حسگر بی سیم است. این شبیه ساز براساس زبان برنامه نویسی جاوا توسعه یافته است و می توان مدل های اعتماد جدید را به آن اضافه نمود.

شرایطی که برای شبیه سازی فرض شده است به این ترتیب می باشد: محدوده ای که گره های حسگر در آن پخش شده اند دارای ابعاد $80m \times 80m$ است، محدوده رادیویی هر گره حسگر برابر $15m$ در نظر گرفته می شود. همچنین $\beta = 0.2$ ، $p = 4$ ، $w_1 = w_2 = 0.5$ ، $\varepsilon = 0.05$ و گره ها به صورت ایستا هستند.

در شبیه سازی ها، مدل اعتماد ۵۰ مرتبه روی ۱۰۰ شبکه حسگر تصادفی که تعداد گره های حسگر در هر یک از شبکه ها برابر N در نظر گرفته می شود، اجرا می گردد (در هر یک از شبکه های مورد آزمون هر کارخواه ۵۰ مرتبه تقاضای سرویس می کند). در هر شبکه تعداد گره های کارخواه ثابت بوده و برابر ۲۵٪ کل گره ها است و ۷۵٪ بقیه به صورت کارپذیر عمل می کنند. درصد کارپذیرهای بدخواه با M نشان داده می شود. در جدول ۱ خلاصه ای از شرایط شبیه سازی آورده شده است.

در بخش های قبل، برای دریافت سرویس از طریق گره ای که بالاترین مقدار اعتماد را دارد اقدام می کند. گره i پس از دریافت سرویس آن را با سرویس مورد تقاضا مقایسه می کند، رضایت گره i از سرویس دریافتی در مرحله n با $S_i(n)$ نشان داده می شود. اگر گره i از سرویس دریافتی راضی باشد مقدار رضایت آن برابر یک و در غیر این صورت مقدار رضایت برابر صفر است. سپس گره i با توجه به رضایت خود از سرویس دریافتی اعتماد گره های همسایه خود را به روز می کند. به روز کردن اعتماد گره های همسایه شامل دو بخش است. بخش اول جریمه یا پاداش گره ای است که دریافت سرویس از طریق آن صورت گرفته و بخش دوم به روز کردن اعتماد گره هایی است که در محاسبه اعتماد غیرمستقیم ظاهر می شوند.

برای جریمه یا پاداش گره ای که دریافت سرویس از طریق آن صورت گرفته است اگر کیفیت سرویس دریافتی مطلوب باشد مقدار اعتماد گره ای که دریافت سرویس از طریق آن صورت گرفته افزایش می یابد و اگر کیفیت سرویس مطلوب نباشد، از مقدار اعتماد آن گره کاسته می شود. فرض می کنیم که گره i اعتماد تمام گره های همسایه اش را به دست آورده و مقدار اعتماد گره j بیشتر از سایر گره ها باشد. در این حالت گره i برای دریافت سرویس از طریق گره j اقدام می کند. پس از دریافت سرویس اگر گره i از سرویس دریافتی رضایت داشته باشد، به گره j پاداش داده و مقدار اعتماد آن را افزایش می دهد و اگر گره i از سرویس دریافتی ناراضی باشد، آن را جریمه می کند و از اعتماد آن گره می کاهد. کاهش یا افزایش اعتماد گره ای که دریافت سرویس از طریق آن صورت گرفته است با رابطه ۳ انجام می پذیرد.

(۳)

$$T_{i,j}(n+1) = \begin{cases} (1 + \beta) * T_{i,j}(n) & S_i(n+1) = 1 \\ (1 - p\beta) * T_{i,j}(n) & S_i(n+1) = 0 \end{cases}$$

در رابطه ۳، β عددی در بازه $[0,1]$ است و p ضریبی برای کنترل نرخ کاهش اعتماد است. $S_i(n+1)$ رضایت گره i از سرویس دریافتی است. i گره تقاضاکننده سرویس و j گره ای است که دریافت سرویس از طریق آن صورت گرفته است.

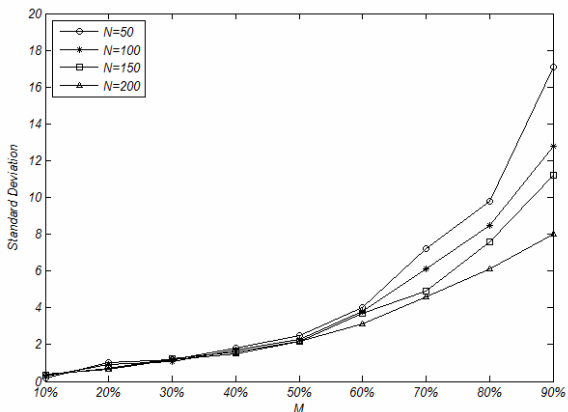
همان طور که اشاره شد هر گره برای محاسبه اعتماد کلی گره های همسایه اش از اعتماد مستقیم و غیرمستقیم استفاده می کند. این گره اعتماد غیرمستقیم را از طریق گره های دیگر به دست می آورد بنابراین منطقی است که پس از دریافت سرویس اعتماد گره هایی که در رابطه اعتماد غیرمستقیم مشارکت داشته اند نیز با توجه به کیفیت سرویس دریافتی افزایش یا کاهش یابد. در صورتی که گره i سرویس مناسبی

کلیه نمودارها مقادیر تقریباً یکسانی دارند و مدل اعتماد پیشنهادی در تمام آن‌ها به یک شکل عمل می‌کند. موضوع دیگری که می‌توان از شکل ۲ استنباط کرد این است که زمانی که درصد گره‌های بدخواه از ۵۰٪ کمتر باشد، درصد انتخاب کارپذیرهای قابل اعتماد بالاتر از ۹۰٪ است. به منظور این‌که مدل اعتماد قابل قبول باشد، باید درصد انتخاب کارپذیرهای قابل اعتماد از اندازه مشخصی، برای مثال ۸۰٪ بیشتر باشد و اگر درصد انتخاب کارپذیرهای قابل اعتماد از این مقدار کمتر باشد نشان‌دهنده ناکارایی مدل است. با توجه به شکل ۲ آزمایشات انجام شده نشان می‌دهد که این مدل اعتماد در حالتی که درصد گره‌های بدخواه افزایش پیدا می‌کند، همچنان به خوبی عمل می‌نماید و تا زمانی که درصد کارپذیرهای بدخواه کمتر از ۷۰٪ باشد، درصد انتخاب کارپذیرهای قابل اعتماد بالاتر از ۸۰٪ است. اما زمانی که تعداد گره‌های بدخواه افزایش یافته و به ۸۰٪ یا بیشتر می‌رسد، بازدهی مدل اعتماد کاهش می‌یابد. از سوی دیگر با توجه به این شکل مشاهده می‌شود که این مشکل در شبکه‌های بزرگ‌تر بیشتر است. بنابراین در شبکه‌های حسگر بی سیم با تعداد کمتر گره، این مدل در حضور درصد بالایی از کارپذیرهای بدخواه همچنان به خوبی عمل می‌کند.

شایان ذکر است با تکرار شبیه‌سازی‌ها و تغییر شرایطی مانند شعاع رادیویی گره‌های حسگر و ابعاد منطقه نتایج مشابهی حاصل شد.

۵-۲- انحراف از میانگین

شکل ۲ میانگین درصد انتخاب کارپذیرهای قابل اعتماد را نشان می‌دهد. اما برای مثال میانگین ۷۰٪ می‌تواند به این دلیل به دست آید که این مدل اعتماد در کلیه شبکه‌ها با N گره، در ۷۰٪ موارد به کارپذیر قابل اعتماد دست می‌یابد و یا این‌که مدل در نیمی از شبکه‌های مورد آزمایش در ۱۰۰٪ موارد به کارپذیر قابل اعتماد دست



شکل ۳: انحراف معیار درصد انتخاب کارپذیرهای قابل اعتماد برای شبکه‌های حسگر با تعداد مختلف گره

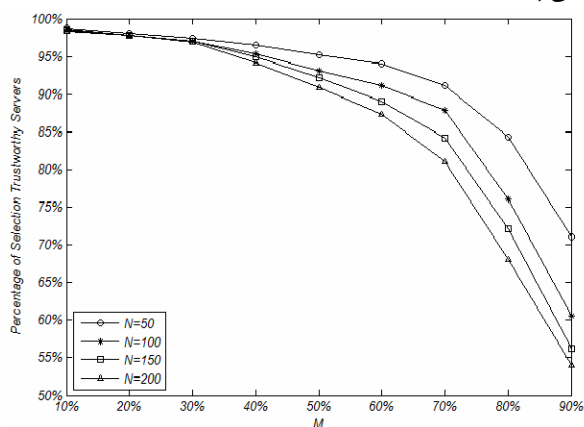
جدول ۱: خلاصه شرایط شبیه‌سازی

N	تعداد گره‌های حسگر
۱۰۰	تعداد شبکه‌های حسگر مورد آزمایش
۵۰	تعداد دفعات اجرای مدل اعتماد روی هر شبکه حسگر
۲۵	تعداد گره‌های کارخواه
۷۵	تعداد گره‌های کارپذیر
M	درصد کارپذیرهای بدخواه

۵-۱- مقیاس پذیری DSTM

از آن‌جا که شبکه‌های حسگر با توجه به کاربرد آن‌ها دارای تعداد مختلفی گره هستند، به بررسی رفتار مدل اعتماد پیشنهادی (DSTM) در شبکه‌های حسگر با تعداد مختلف گره پرداخته می‌شود. به این منظور محاسبات مربوط به مدل DSTM روی شبکه‌های حسگر با $N=50, 100, 150, 200$ و برای هر N روی ۱۰۰ شبکه مختلف اجرا گردید. با تغییر M از ۱۰٪ تا ۹۰٪ در هر شبکه، میزان دستیابی کارخواه‌ها به کارپذیرهای قابل اعتماد اندازه‌گیری شد، به این صورت که هر کارخواه ۵۰ مرتبه تقاضای سرویس می‌کند و میانگین دستیابی کارخواه‌ها به کارپذیرهای قابل اعتماد در ۱۰۰ شبکه مورد آزمون اندازه‌گیری می‌گردد. نتایج شبیه‌سازی‌ها در شکل ۲ نشان داده شده است.

اولین نکته‌ای که با توجه به شکل ۲ ملاحظه می‌شود شباهت بین درصد انتخاب کارپذیرهای قابل اعتماد، صرف‌نظر از اندازه شبکه است، که بیان‌کننده مقیاس‌پذیری مدل اعتماد پیشنهادی است. به این مفهوم که مدل اعتماد پیشنهادی در شبکه‌های با تعداد مختلف



شکل ۲: میزان دستیابی کارخواه‌ها به کارپذیرهای قابل اعتماد در شبکه‌های حسگر با تعداد گره‌های مختلف با تغییر درصد کارپذیرهای بدخواه

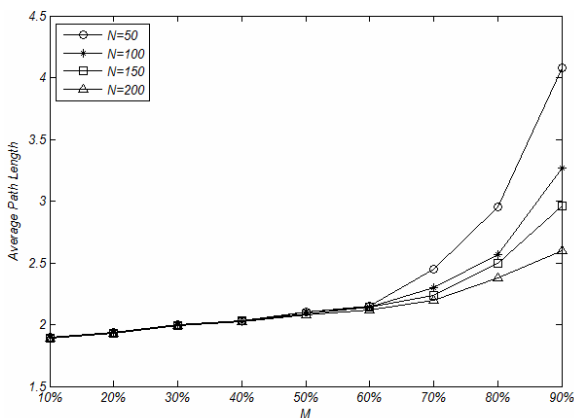
گره حسگر به صورت یکسانی عمل می‌کند به خصوص اگر M (درصد کارپذیرهای بدخواه) در شبکه کمتر از ۴۰٪ باشد

شبکه دارد.

۵-۳- بررسی طول مسیر

برای بررسی طول مسیر و تأثیر اندازه شبکه روی آن در شرایط قبل شبیه‌سازی انجام شده و در هر مورد تعداد پرش‌های مسیره‌های منتهی‌شونده به کارپذیرهای قابل اعتماد توسط این مدل به دست آمد، و نتیجه حاصل به صورت شکل ۵ است.

با توجه به شکل ۵ می‌توان دید که در حالتی که درصد کارپذیرهای بدخواه کمتر از ۶۰٪ است در کلیه شبکه‌ها متوسط طول مسیر کوتاه است. همان‌طور که مشاهده می‌شود طولانی‌ترین مسیر متوسط در شرایطی است که تعداد گره‌های حسگر برابر ۵۰ است و درصد گره‌های بدخواه نیز ۹۰٪ می‌باشد. با توجه به نتایج به دست آمده، مدل اعتماد پیشنهادی می‌تواند صرف‌نظر از اندازه شبکه و درصد کارپذیرهای بدخواه، به کارپذیرهای قابل اعتماد دست یابد از این‌رو مقیاس پذیر است.

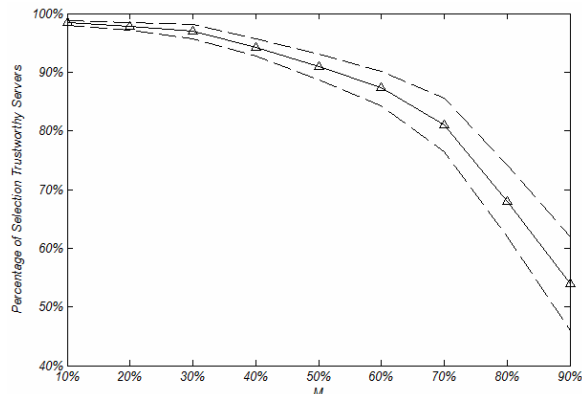


شکل ۵: متوسط تعداد پرش‌های منتهی‌شونده به کارپذیرهای قابل اعتماد

۶- نتیجه‌گیری!

شبکه‌های حسگر بی سیم، از تعدادی گره حسگر تشکیل شده‌اند و معمولاً برای پایش شرایط محیطی و فیزیکی به کار می‌روند. هرچند نیازمندی‌های امنیتی این شبکه‌ها مشابه سایر شبکه‌ها می‌باشد، راه‌حل‌های امنیتی آن‌ها به دلیل خصوصیات شبکه‌های حسگر نسبتاً متفاوت است. مدل‌های اعتماد که اعتماد را در رفتار عناصر شبکه مدل می‌کنند به خصوص برای شبکه‌های حسگر بی سیم مفید هستند.

در این مقاله یک مدل اعتماد توزیع شده و مقیاس‌پذیر به نام DSTM برای شبکه‌های حسگری که به صورت کارخواه و کارپذیر می‌باشند پیشنهاد شد که در آن هر گره اعتماد همسایه‌های خود را نگهداری می‌کند و این اعتماد را براساس



شکل ۴: مقدار نوسانات دستیابی به کارپذیرهای قابل اعتماد در ۱۰۰ شبکه مورد آزمون متشکل از ۲۰۰ گره

می‌یابد و در نیم دیگر شبکه‌ها در ۴۰٪ موارد کارپذیر قابل اعتماد را به دست می‌آورد. به منظور راست‌آزمایی نتایج حاصل از شبیه‌سازی انحراف معیار تمام منحنی‌ها اندازه‌گیری شد که در شکل ۳ نشان داده شده است. به منظور وضوح بیشتر برای $N = 200$ به عنوان نمونه در شکل ۴ مجدداً درصد دستیابی به کارپذیرهای قابل اعتماد بر حسب M نمایش داده شده است که حاکی از نوسانات کم و قابل قبول می‌باشد.

در شکل ۳ نیز اولین موضوع قابل توجه، شباهت کلیه نمودارهایی است که برای شبکه‌های حسگر با N های مختلف به دست آمده است. به خصوص در حالتی که درصد گره‌های بدخواه کمتر از ۵۰٪ باشد، انحراف معیار عدد کوچکی بوده و برای تمامی نمودارها مقدار تقریباً یکسانی دارد. این موضوع بدان معنی است که زمانی که درصد کارپذیرهای بدخواه در شبکه کمتر از ۵۰٪ باشد، مدل اعتماد پیشنهادی می‌تواند با توجه به شکل ۲ در شبکه‌های با تعداد مختلف گره به کارپذیرهای قابل اعتماد دست یابد، بدون این‌که به ساختار آن‌ها وابسته باشد.

با توجه به شکل ۳، زمانی که M افزایش می‌یابد نمودارها از یکدیگر فاصله گرفته و برای شبکه‌های کوچک‌تر، انحراف معیار با افزایش M رشد بیشتری دارد به این مفهوم که در شبکه‌های با N کمتر مدل اعتماد پیشنهادی به ساختار شبکه تحت آزمایش وابسته است.

به طور خلاصه می‌توان بیان کرد اگر تعداد گره‌های تشکیل‌دهنده شبکه کم و حدود ۵۰ گره باشد، وابستگی این مدل اعتماد به ساختار شبکه و چگونگی قرار گرفتن گره‌ها نسبت به یکدیگر بیشتر از حالتی است که تعداد گره‌های تشکیل‌دهنده شبکه زیاد و حدود ۲۰۰ گره است. از این رو برای شبکه‌های بزرگ این مدل اعتماد وابستگی کمتری به ساختار

- Economics of Peer-to-Peer Systems, pp. 83-89, 2004.
- [8] Y. Sun, Y. Yang, "Trust Establishment in Distributed Networks: Analysis and Modeling", Proceedings of the IEEE International Conference on Communications and Information Systems Security Symposium, pp. 1266-1273, 2007.
- [9] Zh. Liu, W. Joy, R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks", Proceeding of the IEEE International Workshop on Future Trends of Distributed Computing Systems, pp 80-85, 2004.
- [10] F. Gómez, G. Martínez, "TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks", in Proceeding of the Communication and Information Systems Security Symposium, pp. 545-552, 2009.

کیفیت سرویس‌های دریافتی و به صورت تکاملی در هر مرحله به روز و به مقدار واقعی نزدیک می‌کند. DSTM دارای مزایایی است از جمله این‌که در این مدل گره‌های حسگر فقط اعتماد همسایه‌های خود را نگه می‌دارند و بنابراین حافظه مورد نیاز و حجم محاسبات مربوط به اعتماد محدود شده و به همین دلیل تعداد کل گره‌های شبکه بر عملکرد آن تأثیری ندارد از این‌رو مدل پیشنهادی مقیاس پذیر است. شبیه‌سازی‌ها نشان می‌دهد که اگر تعداد کارپذیرهای بدخواه در شبکه، کمتر از 50% کل کارپذیرها باشد صرف نظر از تعداد گره‌های شبکه، میزان دستیابی کارخواه‌ها به کارپذیرهای قابل اعتماد بالاتر از 90% است.

از آن‌جا که شبکه‌های حسگر در معرض حمله گره‌های بدخواه قرار دارند، در آینده می‌توان مقاومت این مدل اعتماد را در برابر حملات بررسی کرد. همچنین در این مدل اعتماد سرویس‌ها با یک شناسه یا نام مشخص می‌شوند که در آینده می‌توان آن‌ها را براساس خصوصیاتمانند هزینه، کیفیت و ارزشمند بودن مشخص کرد.

7- سپاسگزاری

این پژوهش در دانشکده مهندسی برق دانشگاه علم و صنعت ایران با حمایت مرکز تحقیقات مخابرات ایران انجام گردیده است. بدین وسیله از حمایت‌های آن مرکز تقدیر و سپاسگزاری می‌گردد.

8- مراجع

- [1] F. Gómez M'armol, G. Martínez Pérez, "Providing Trust in Wireless Sensor Networks using a Bio-inspired Technique", Proceedings of the Networking and Electronic Commerce Research Conference, pp. 312-321, 2008.
- [2] G. Han, L. Shu, J. Hyuk Park, J. Ni, "Power-Aware and Reliable Sensor Selection Based on Trust for Wireless Sensor Networks", Journal of Communications, pp- 23-30, 2010.
- [3] T. Zahariadis, E. Ladis, H.C.Leligou, P. Trakadas, C. Tselikis, K. Papadopoulos, "Trust Models for Sensor Networks", International Symposium ELMAR, pp. 281-290, 2008.
- [4] D. Artz, Y. Gil, "A Survey of Trust in Computer Science and the Semantic Web", Proceeding of the Web Semantics: Science, Services and agent on the world wide web, pp. 58-71, 2007.
- [5] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities", IEEE Transactions on Knowledge and Data Engineering, pp. 843-857, 2004.
- [6] S. Ganeriwal, M. Srivastava, "Reputation-based Framework For High Integrity Sensor Networks", Proceeding of the ACM workshop on Security of Ad-hoc and Sensor networks, pp.66-77, 2004.
- [7] S. Buchegger, J. Y. Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks", Proceedings of the Workshop on the