هفتمین کنفرانس بین المللی انجمن رمز ایران
۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی
دانشگاه صنعتی خواجه نصیرالدین طوسی
انجمن رمزایران

مدیریت اعتماد توزیع‌شده و مقیاس‌پذیر در شبکه‌های حسگر بی‌سیم

خدیجه نخعی[۱]، هادی‌شهریار شاه‌حسینی[۲]
دانشگاه علم و صنعت ایران، دانشکده برق[۱و۲]
hshsh@iust.ac.ir

چکیده

راه‌حل‌های امنیتی که برای شبکه‌های حسگر پیشنهاد شده‌اند اغلب با فرض وجود یک محیط قابل اعتماد به وجود آمده‌اند، در حالی که معمولاً این گونه نیست. بنابراین مدیریت اعتماد نیاز اساسی ارائه راه‌حل‌های امنیتی در شبکه‌هاست. طرح‌های مدیریت اعتماد موجود که برای سایر شبکه‌ها طراحی شده‌اند، برای شبکه‌های حسگر مناسب نیستند زیرا مقدار زیادی انرژی و حافظه مصرف می‌کنند. از سوی دیگر شبکه‌های حسگر معمولاً دارای تعداد زیادی گره می‌باشند و این مسئله باعث می‌شود مقیاس‌پذیری مدل اعتماد از اهمیت خاصی برخوردار باشد. در این مقاله مدل اعتماد توزیع‌شده‌ای برای شبکه‌های حسگر بیسیم پیشنهاد می‌شود که در آن هر گره از دو منبع اعتماد مستقیم و غیرمستقیم برای محاسبه اعتماد استفاده می‌کند و از طرف دیگر هر گره تنها اعتماد گره‌های همسایه خود را نگه می‌دارد، از این رو به ساختار کلی شبکه و تعداد گره‌های آن وابسته نیست و بنابراین مقیاس‌پذیر است. شبیه‌سازی‌ها نشان می‌دهند که مدل اعتماد پیشنهادی صرف‌نظر از تعداد گره‌های شبکه رفتار مشابهی در کلیه آن‌ها دارد و اگر تعداد کارپذیرهای بدخواه کمتر از ۵۰٪ کل کارپذیرها باشد، میزان دستیابی کارخواه‌ها به کارپذیرهای قابل اعتماد در شبکه‌های با تعداد مختلف گره حسگر بیشتر از ۹۰٪ است.

واژه های کلیدی

مدل اعتماد، اعتماد مستقیم، اعتماد غیرمستقیم، شبکه حسگر بی‌سیم.

۱- مقدمه

شبکه‌های حسگر بی‌سیم شبکه‌هایی براساس همکاری گره‌های کوچک می‌باشند. این گره‌ها اساساً با مصرف انرژی کم، هزینه اندک و ارتباطات بیسیم مشخص می‌شوند. آن‌ها می‌توانند برای اندازه‌گیری دما، فشار، رطوبت، نور و ... به کار روند، اما دارای محدودیت‌هایی مانند محدودیت حافظه، قدرت محاسباتی و انرژی هستند[۱]. این شبکه‌ها با توجه به کاربرد آن‌ها دارای تعداد مختلف گره حسگر می‌باشند.

شبکه‌های حسگر به صورت موقتی شکل می‌گیرند و توسط خود گره‌ها سازماندهی می‌شوند. در یک شبکه حسگر پیچیده، گره‌های بدخواه به خوبی تغییر شکل می‌دهند و می‌توانند با استفاده از خصوصیت ذاتی مشارکت شبکه‌های حسگر به عناصر شبکه حمله کنند. همچنین این خصوصیت شبکه‌های حسگر بیسیم که مستعد خطا می‌باشند، باعث ناپایداری این شبکه‌ها می‌گردد. بنابراین چگونگی انتخاب گره‌های همکار در تراکنش‌ها برای افزایش بازده اهمیت زیادی پیدا می‌کند[۲]. مدل‌های اعتماد ابزار مناسبی برای دستیابی به این هدف می‌باشند.

مفهوم مدیریت اعتماد، که اعتماد را در اجزای شبکه مدل می‌کند، می‌تواند برای این شبکه‌ها مفید باشد. اعتماد علاوه بر آن‌که می‌تواند در مورد خودسازمان‌دهی گره‌های شبکه در برابر تغییرات رخ داده در همسایگی آن‌ها کمک کند، می‌تواند در برقراری پروتکل‌های امنیتی نیز شرکت کند. یک سامانه مدیریت اعتماد می‌تواند برای آشکارسازی گره‌هایی که به درستی رفتار نمی‌کنند نیز مفید باشد، و یا می‌تواند در تصمیم‌گیری به گره‌ها کمک کند[۳].

با توجه به اهمیت اعتماد در شبکه‌های حسگر بی‌سیم از یک سو و از سوی دیگر محدودیت‌هایی مانند محدودیت انرژی، حافظه و قدرت محاسباتی و تعداد قابل توجه گره حسگر مسأله مهم چگونگی محاسبه اعتماد گره‌ها مطرح است[۴]. بر این اساس ارائه مدل اعتماد مقیاس‌پذیر براساس محدودیت‌های این شبکه‌ها از اهمیت خاصی برخوردار است.

در این مقاله مدل اعتماد توزیع‌شده‌ای معرفی می‌شود که گره‌ها برای محاسبه اعتماد یکدیگر از دو منبع آزمایش‌های مستقیم و غیرمستقیم استفاده می‌کنند و هر گره فقط مقادیر اعتماد همسایه‌های خود را نگه می‌دارد و بیش از این در مورد تعداد گره‌های تشکیل دهنده شبکه نمی‌داند. این توزیع‌شدگی و نحوه محاسبه اعتماد باعث می‌شود که روش پیشنهاد شده مقیاس‌پذیر باشد و به این دلیل DSTM[1] نامیده شده است.

در ادامه این مقاله، در بخش دوم به بررسی اجمالی برخی از مدل‌های اعتماد موجود برای شبکه‌های حسگر بی سیم پرداخته می‌شود، بخش سوم به توصیف کلی مدل اعتماد پیشنهادی (DSTM) اختصاص دارد. در بخش چهارم چگونگی به روز شدن مقادیر اعتماد گره‌ها مطرح می‌شود. بخش پنجم شبیه‌سازی‌ها را ارائه می‌دهد و در بخش ششم نیز نتیجه‌گیری و کارهای آینده بیان خواهد شد.

۲- مروری بر کارهای پیشین!

روش‌های اعتماد و اعتبار ابزار مهمی هستند که در بسیاری از زمینه‌ها مانند اجتماعی، اقتصادی و علوم کامپیوتر مورد استفاده قرار می‌گیرند. سیستم‌های اعتماد روش مفیدی برای تشخیص تهدیدات اعضای فریبکار یا اعضای در خطر افتاده یک شبکه هستند. این سیستم‌ها با شناسایی گره‌های بدخواه و حذف آن‌ها از شبکه کار خود را انجام می‌دهند[۵].

RFSN [۶] اولین مدل اعتمادی است که منحصراً برای شبکه‌های حسگر بی سیم طراحی و گسترده شده است و از روش سگ نگهبان[2] برای ایجاد اعتماد استفاده می‌کند. اما سگ نگهبان به خاطر نقایص خودش نمی‌تواند تمام رفتارها را ثبت کند و بنابراین مقداری نامعینی در این سیستم وجود دارد.

ATRM [۷] یک طرح مدیریت اعتماد برای شبکه‌های حسگر بی سیم براساس عامل است که مدیریت اعتماد به صورت محلی و با سرباره کمی از نظر پیام و تأخیر اجرا می‌شود ولی از جمله معایب این مدل این است که یک موجودیت مورد اعتماد مسئول ایجاد و حفظ عامل‌ها می‌باشد و همچنین عامل‌ها در برابر تحلیل‌های غیرمجاز و اصلاح منطق محاسباتی آن‌ها آسیب‌پذیرند.

ATSN [۸] مدلی است که گره‌های حسگر اعتماد دیگر گره‌های شبکه را نگه می‌دارند. یک گره مسئولیت پایش سایر گره‌ها را به عهده دارد و اعتبار آن‌ها را به دست می‌آورد و از این اعتبار برای ارزیابی قابلیت اعتماد و پیش‌بینی رفتار آینده استفاده می‌کند. در زمان تراکنش هر گره فقط با گره‌هایی که به آن‌ها اعتماد دارد همکاری می‌کند.

در مدلی که در این مقاله معرفی می‌شود هر گره مقدار اعتماد گره‌هایی را که در محدوده رادیویی آن قرار دارند، براساس تراکنش‌های قبلی و از دو طریق به دست می‌آورد. این مدل نیاز به یک مرکز اعتماد برای نگه‌داری مقادیر اعتماد ندارد که به خوبی با شبکه‌های حسگر بی سیم سازگار است.

۳- فرضیات و توصیف کلی DSTM!

شبکه‌های حسگر بی سیم با توجه به نوع گره‌های تشکیل‌دهنده آن‌ها دارای انواع مختلفی هستند. در یک دسته‌بندی، شبکه‌های حسگر به دو دسته ایستا و پویا تقسیم می‌شوند، در شبکه‌های ایستا گره‌ها مکان مشخصی دارند در حالی که در شبکه‌های پویا، گره‌ها به هر جایی حرکت می‌کنند. در این مقاله شبکه‌های حسگر به صورت ایستا هستند. برای فراهم کردن شرایط مورد نیاز در شبیه‌سازی‌ها فرض می‌شود برخی از گره‌ها تقاضاکننده سرویس (یا کارخواه[3]) هستند و برخی دیگر فراهم‌آورنده سرویس (یا کارپذیر[4]) هستند. همچنین فرض می‌شود که هر گره فقط همسایه‌های خود را که در محدوده رادیویی آن هستند می‌شناسد و هیچ چیز در مورد ساختار کلی شبکه نمی‌داند.

در مدل اعتماد پیشنهادی (DSTM)، گره‌ها برای به دست آوردن مقدار اعتماد همسایه‌های خود از دو منبع اعتماد مستقیم و اعتماد غیرمستقیم استفاده می‌کنند، هر گره مقادیر اعتماد مستقیم گره‌هایی که در محدوده رادیویی آن قرار دارند را می‌داند و علاوه بر آن در مورد هر یک از گره‌ها از اعتماد غیرمستقیمی‌که توسط سایر گره‌ها به دست می‌آورد استفاده می‌کند و سپس با ترکیب اعتماد مستقیم و غیرمستقیم یک مقدار اعتماد کلی برای هر گره محاسبه می‌کند. مقدار اعتماد برای هر گره به صورت عددی در بازه [۰،۱] می‌باشد.

در ادامه به بیان جزئیات این مدل پرداخته می‌شود و چگونگی محاسبه اعتماد مستقیم و غیر مستقیم و ترکیب آن‌ها برای به دست آوردن اعتماد کلی بیان می‌شود.

---

[1] Distributed & Scalable Trust Model

[2] Watchdog

[3] Client

[4] Server

۳-۱- اعتماد مستقیم!

در مرحله راه‌اندازی سامانه مدیریت اعتماد باید برای هر گره مقدار اعتماد اولیه‌ای در نظر گرفت. اگر مقدار اعتماد اولیه گره‌ها به یکدیگر زیاد و نزدیک به یک باشد همه گره‌ها 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 می‌شویم[۹]. از این رو مقدار اعتماد مستقیم هر گره برای گره‌های همسایه‌اش برابر ۰/۵ است و در طول تراکنش‌های مختلف این مقدار اعتماد به روز و به مقدار واقعی نزدیک می‌شود.

همان‌طور که قبلاً بیان شد هر گره اعتماد سایر گره‌ها که در محدوده رادیویی آن قرار دارند را نگه می‌دارد، از این رو گره‌ها برای نگهداری مقادیر اعتماد به حافظه کمتری در مقایسه با مدل‌های اعتماد توزیع‌شده نیاز دارد [۱۰]. این موضوع با توجه به شکل ۱ مشخص می‌شود. در این شکل گره ۱ مقدار اعتماد گره‌های ۲، ۳، ۴ و ۶ را نگه می‌دارد. مقدار اعتماد مستقیم یک گره به گره دیگر در مرحله n با $T_{i,j}(n)$ که $i, j = 1,2,3,...$ نشان داده می‌شود.

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 گره‌ها در مورد گره j دارند استفاده کند. ولی تنها گره‌هایی می‌توانند به گره i در به دست آوردن اعتماد غیرمستقیم کمک کنند، که گره j در محدوده رادیویی آن‌ها 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 گره‌های همسایه‌اش را نگه‌داری می‌کند. در شکل ۱ گره‌های ۳ و ۴ در محدوده رادیویی مشترک گره‌های ۱ و ۲ قرار دارند، بنابراین گره ۱ برای به دست آوردن اعتماد غیرمستقیم گره ۲ از این دو گره استفاده می‌کند. اما گره‌هایی مانند گره ۶ که در محدوده رادیویی گره ۲ نیست و همچنین گره ۵ که در محدوده رادیویی گره ۲ می‌باشد ولی در محدوده رادیویی گره ۱ قرار نمی‌گیرد در رابطه اعتماد غیرمستقیم وارد نمی‌شوند. اعتماد غیرمستقیم گره i به گره j در مرحله n با $R_{i,j}(n)$ نشان داده می‌شود.

اگر گره i بخواهد مقدار اعتماد غیرمستقیم گره j را به دست آورد، از گره‌های همسایه‌اش مقدار اعتماد مستقیم گره j را سؤال می‌کند و با توجه به اعتمادی که خودش در مورد گره‌های پاسخ‌دهنده دارد اعتماد غیرمستقیم گره j را به صورت زیر محاسبه می‌کند.

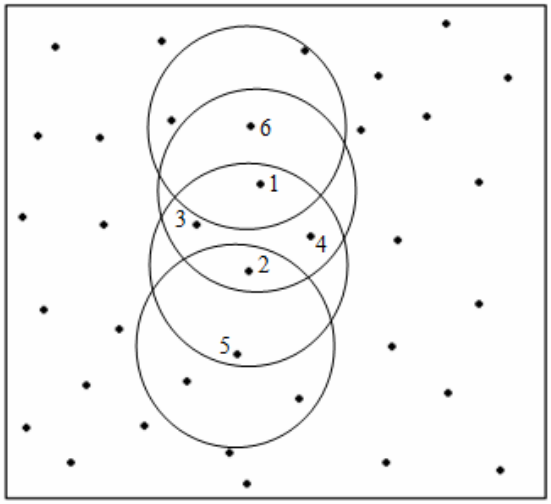
$$R_{i,j}(n) = \frac{1}{N}\sum_{k} T_{i,k} * T_{k,j}$$

در رابطه (۱)، N تعداد گره‌های موجود در محدوده مشترک بین گره i و j است و k شماره آن گره‌ها 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 می‌کند و یک مقدار اعتماد کلی برای هر یک از همسایگانش به دست می‌آورد. مقدار اعتماد کلی گره i به گره j با $T'_{i,j}$ نشان داده می‌شود و از رابطه ۲ به دست می‌آید.

$$T'_{i,j}(n) = w_1 T_{i,j}(n) + w_2 R_{i.j}(n) \qquad (۲)$$



شکل ۱: گره ۱ اعتماد مستقیم گره‌های ۲، ۳، ۴ و ۵ را نگه می‌دارد. این گره برای به دست آوردن اعتماد غیرمستقیم گره ۲ از گره‌های ۳ و ۴ کمک می‌گیرد.

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 گره‌ها تغییر می‌کنند.

۴- به روز کردن مقدار اعتماد!

به روز کردن مقدار اعتماد گره‌ها به رضایت گره تقاضاکننده از سرویس دریافتی، بستگی دارد. سرویس با یک نام یا شناسه مشخص می‌شود. اگر گره i سرویسی را درخواست کرده باشد، پس از محاسبه اعتماد گره‌های همسایه‌اش به روش بیان‌شده

در بخش‌های قبل، برای دریافت سرویس از طریق گره‌ای که بالاترین مقدار اعتماد را دارد اقدام می‌کند. گره i پس از دریافت سرویس آن را با سرویس مورد تقاضا مقایسه می‌کند، رضایت گره i از سرویس دریافتی در مرحله n با $S_i(n)$ نشان داده می‌شود. 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 گره‌های همسایه خود را به روز می‌کند.

به روز کردن اعتماد گره‌های همسایه شامل دو بخش است. بخش اول جریمه یا پاداش گره‌ای است که دریافت سرویس از طریق آن صورت گرفته و بخش دوم به روز کردن اعتماد گره‌هایی است که در محاسبه اعتماد غیرمستقیم ظاهر می‌شوند.

برای جریمه یا پاداش گره‌ای که دریافت سرویس از طریق آن صورت گرفته است اگر کیفیت سرویس دریافتی مطلوب باشد مقدار اعتماد گره‌ای که دریافت سرویس از طریق آن صورت گرفته افزایش می‌یابد و اگر کیفیت سرویس مطلوب نباشد، از مقدار اعتماد آن گره کاسته می‌شود. فرض می‌کنیم که گره i اعتماد تمام گره‌های همسایه‌اش را به دست آورده و مقدار اعتماد گره j بیشتر از سایر گره‌ها باشد. در این حالت گره i برای دریافت سرویس از طریق گره j اقدام می‌کند. پس از دریافت سرویس اگر گره i از سرویس دریافتی رضایت داشته باشد، به گره j پاداش داده و مقدار اعتماد آن را افزایش می‌دهد و اگر گره i از سرویس دریافتی ناراضی باشد، آن را جریمه می‌کند و از اعتماد آن گره می‌کاهد. کاهش یا افزایش اعتماد گره‌ای که دریافت سرویس از طریق آن صورت گرفته است با رابطه ۳ انجام می‌پذیرد.

(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 [۰،۱] 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 گره‌ای است که دریافت سرویس از طریق آن صورت گرفته است.

همان‌طور که اشاره شد هر گره برای محاسبه اعتماد کلی گره‌های همسایه‌اش از اعتماد مستقیم و غیرمستقیم استفاده می‌کند. این گره اعتماد غیرمستقیم را از طریق گره‌های دیگر به دست می‌آورد بنابراین منطقی است که پس از دریافت سرویس اعتماد گره‌هایی که در رابطه اعتماد غیرمستقیم مشارکت داشته‌اند نیز با توجه به کیفیت سرویس دریافتی افزایش یا کاهش یابد. در صورتی که گره i سرویس مناسبی دریافت کرده باشد مقدار اعتماد تمامی گره‌هایی که در رابطه اعتماد غیرمستقیم ظاهر شده‌اند را به میزان بسیار کمی افزایش می‌دهد و برعکس اگر کیفیت سرویس دریافتی در حد مطلوب نباشد گره i مقدار اعتماد این گره‌ها را مقدار بسیار کمی کاهش خواهد داد. کاهش یا افزایش اعتماد گره‌های سهیم در محاسبه اعتماد غیرمستقیم توسط رابطه ۴ صورت می‌گیرد.

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

در رابطه ۴، ε بسیار کوچکتر از β است زیرا نمی‌توان از روی کیفیت سرویس دریافتی قضاوت کاملی در مورد تمام این گره‌ها داشت و مقدار اعتماد آن‌ها نباید تغییر چشمگیری داشته باشد. k گره‌هایی هستند که در رابطه محاسبه اعتماد غیر مستقیم گره i در مورد j ظاهر می‌شوند.

۵- شبیه‌سازی!

برای ارزیابی DSTM از شبیه‌سازی با نرم‌افزار TRMSim-WSN استفاده شده است[۱۰]. TRMSim-WSN یک شبیه‌ساز دامنه آزاد مدل‌های اعتماد و اعتبار برای شبکه‌های حسگر بی سیم است. این شبیه‌ساز براساس زبان برنامه‌نویسی جاوا توسعه یافته است و می‌توان مدل‌های اعتماد جدید را به آن اضافه نمود.

شرایطی که برای شبیه‌سازی فرض شده است به این ترتیب می‌باشد: محدوده‌ای که گره‌های حسگر در آن پخش شده‌اند دارای ابعاد $80m\times80m$ است، محدوده رادیویی هر گره حسگر برابر $15m$ در نظر گرفته می‌شود. همچنین $\beta=0.2$ ، $p=4$ ، $w_1=w_2=0.5$ ، $\varepsilon=0.05$ و گره‌ها به صورت ایستا هستند.

در شبیه‌سازی‌ها، مدل اعتماد ۵۰ مرتبه روی ۱۰۰ شبکه حسگر تصادفی که تعداد گره‌های حسگر در هر یک از شبکه‌ها برابر N در نظر گرفته می‌شود، اجرا می‌گردد (در هر یک از شبکه‌های مورد آزمون هر کارخواه ۵۰ مرتبه تقاضای سرویس می‌کند). در هر شبکه تعداد گره‌های کارخواه ثابت بوده و برابر ۲۵٪ کل گره‌ها است و ۷۵٪ بقیه به صورت کارپذیر عمل می‌کنند. درصد کارپذیرهای بدخواه با M نشان داده می‌شود. در جدول ۱ خلاصه‌ای از شرایط شبیه‌سازی آورده شده است.

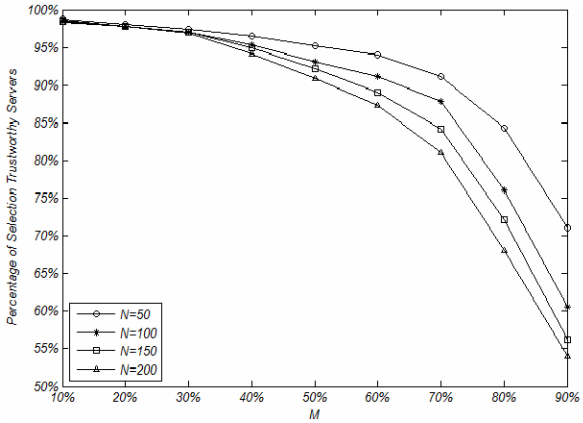
جدول ۱: خلاصه شرایط شبیه‌سازی

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

۵-۱- مقیاس‌پذیری 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. بـه این مفهوم که مـدل اعتماد پیشنهـادی در شبکه‌های بـا تعداد مختلف



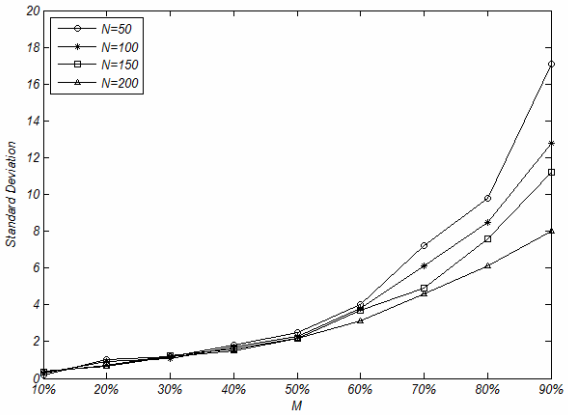
شکل ۲: میزان دستیابی کارخواه‌ها به کارپذیرهای قابل اعتماد در شبکه‌های حسگر با تعداد گره‌های مختلف با تغییر درصد کارپذیرهای بدخواه

گره حسگر به صورت یکسانی عمل می‌کند به خصوص اگر M (درصد کارپذیرهای بدخواه) در شبکه کمتر از ۴۰٪ باشد کلیه نمودارها مقادیر تقریبا یکسـانی دارند و مدل اعتماد پیـشنهادی در تمام آن‌ها به یک شکل عمل می‌کند. موضوع دیگری که می‌توان از شکل ۲ استنباط کرد این است که زمانی‌که 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 زمانی‌که 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.

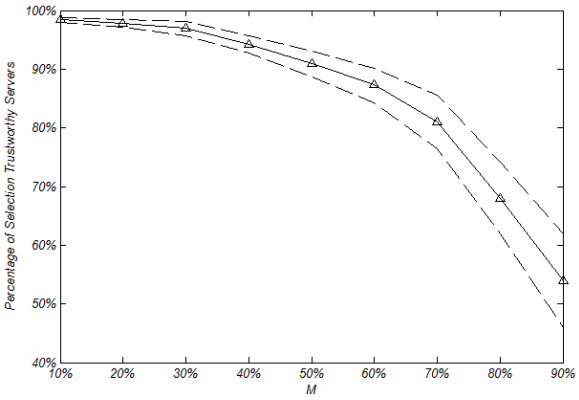
شایان ذکر است با تکرار شبیه‌سازی‌ها و تغییر شرایطی مانند شعاع رادیویی گره‌های حسگر و ابعاد منطقه نتایج مشابهی حاصل شد.

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 نیمـی از شبکـه‌های مـورد 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



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 زمانی‌که 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، زمانی‌که 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.

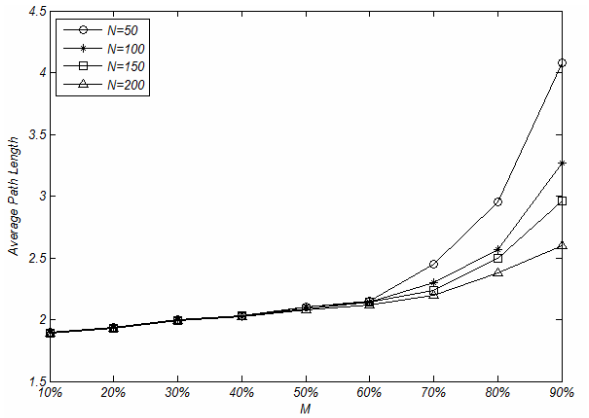
به طور خلاصه می‌توان بیان کرد اگر تعداد گره‌های تشکیل‌دهنده شبکه کم و حدود ۵۰ گره باشد، وابستگی این مدل اعتماد به ساختار شبکه و چگونگی قرار گرفتن گره‌ها نسبت به یکدیگر بیشتر از حالتی است که تعداد گره‌های تشکیل‌دهنده شبکه زیاد و حدود ۲۰۰ گره است. از این رو برای شبکه‌های بزرگ این مدل اعتماد وابستگی کمتری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

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 خصوصیاتی مانند 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. G´omez M´armol, G. Mart´ınez P´erez, “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 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.