علوم و مهندسی کامپیوتر
نشریه علمی پژوهشی انجمن کامپیوتر ایران
مجلد ۷، شماره ۱ و ۳ (الف)، ۱۳۸۸
صفحات ۱۶-۲۱
مقاله کوتاه

مدل اعتماد توزیع‌شده و مقیاس‌پذیر در شبکه‌های حسگر بی‌سیم و ارزیابی و تحلیل کارایی آن

خدیجه نخعی هادی شهریار شاه‌حسینی

دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران، ایران

چکیده

اکثر روش‌هائی که سعی در افزایش کارآئی و عمر شبکه‌های حسگر دارند بر مبنای داشتن یک محیط قابل اعتماد بنا شده‌اند. مدل‌های اعتماد کمک می‌کنند تا گره‌های شبکه به صورت موثرتری گره‌های بدخواه را از گره‌های عادی تشخیص دهند. از آن‌جا که شبکه‌های حسگر معمولاً دارای تعداد زیادی گره می‌باشند، مقیاس‌پذیری در مدل اعتماد از اهمیت خاصی برخوردار است. در این مقاله یک مدل اعتماد توزیع شده و مقیاس‌پذیر برای شبکه‌های حسگر پیشنهاد شده است. در روش پیشنهادی برای محاسبه اعتماد هر گره، از ترکیب اعتماد مستقیم و غیرمستقیم تعداد محدودی از گره‌های همسایه‌ی گره موردنظر استفاده می‌شود. کارایی مدل پیشنهادی به کمک شبیه سازی و روابط تحلیلی، مورد ارزیابی قرار می‌گیرد. ملاحظه خواهد شد که نحوه توزیع‌شدگی این مدل امکان کنترل حافظه مورد نیاز گره‌ها و ترافیک ناشی از محاسبه اعتماد را فراهم می‌کند. همچنین شبیه‌سازی‌ها نشان می‌دهند که مدل اعتماد پیشنهادی صرف‌نظر از تعداد کل گره‌های شبکه رفتار مشابهی در تمام آن‌ها دارد.

کلمات کلیدی: اعتماد مستقیم، اعتماد غیرمستقیم، مدلسازی تحلیلی، شبکه‌های 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].

با توجه به این‌که شبکه‌های حسگر اغلب بدون زیرساخت می‌باشند و در محیط‌های باز گسترش می‌یابند، در برابر حملات گره‌های بدخواه مانند استراق سمع[۱]، اخلال در سرویس[۲]، تبانی[۳] و رفتار نوسانی[۴] آسیب‌پذیرند [۲].

مطالعات اخیر می‌کوشند که روشی برای احراز هویت شبکه‌های حسگر به منظور جلوگیری از این حملات بیابند [۳، ۴]. پیشنهاد آن‌ها برای امنیت، استفاده از کدهای احراز هویت پیام[۵] و طرح‌های از پیش توزیع شده کلید احتمالی می‌باشد. این رویکردها از جعل هویت‌های ساده یک گره حسگر ممانعت می‌کند اما نمی‌تواند از تزریق داده‌ی نادرست یا جعلی توسط گره‌های بدخواه ممانعت کنند.

بنابراین یک طرح مدیریت اعتماد هوشمند نیاز است که قابلیت اعتماد گره‌های حسگر را به منظور تفاوت قائل شدن بین گره‌های بدخواه و گره‌های بی‌ضرر تشخیص دهد، و گره‌های قابل اعتماد را قوی و گره‌های مشکوک را ضعیف‌تر کند [۵].

در این مقاله یک مدل اعتماد توزیع‌شده معرفی می‌شود که گره‌ها برای محاسبه اعتماد یکدیگر از اعتماد 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[۶] نامیده شده است.

در ادامه این مقاله، در بخش دوم به بررسی اجمالی برخی از مدل‌های اعتماد

موجود برای شبکه‌های حسگر بیسیم پرداخته می‌شود، در بخش سوم فرضیات مورد نیاز برای مدل اعتماد پیشنهادی بیان می‌شود، بخش چهارم به تحلیل و ارزیابی DSTM اختصاص دارد، توزیع‌شدگی و مقیاس‌پذیری مدل اعتماد پیشنهادی در این بخش بررسی خواهد شد. در پایان و در بخش پنجم نتیجه‌گیری و کارهای آینده آورده می‌شوند.

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 [۶].

سیستم PowerTrust [۷]، با استفاده از یک روش امتیازدهی توزیع‌شده، تعدادی گره قابل اعتماد که بیشترین انرژی را دارند تحت عنوان گره انرژی به صورت متناوب انتخاب می‌کند. در این مدل اعتماد، ابتدا یک شبکه پوششی اعتماد براساس گره‌های تشکیل دهنده شبکه ایجاد می‌شود. کلیه گره‌ها زمانی که یک تراکنش بین یک جفت گره اتفاق می‌افتد، یکدیگر را ارزیابی می‌کنند. بنابراین گره‌ها مقادیر اعتماد محلی را به صورت متناوب بین خودشان ارسال می‌کنند. این مقادیر، به عنوان ورودی سیستم PowerTrust هستند. وظیفه سیستم PowerTrust جمع‌آوری مقادیر اعتماد محلی و محاسبه اعتماد کلی هر گره است. کلیه امتیازهای عمومی یک بردار اعتماد به صورت $V=(v_1,v_2....,v_n)$ را تشکیل می‌دهند که خروجی سیستم PowerTrust است.

در EigenTrust [۸]، هر گره i تعداد تراکنش‌های رضایت‌بخش و بدون رضایت با گره j را نگه می‌دارد و با استفاده از آن‌ها، مقدار اعتماد محلی گره j را به مقدار $c_{i,j}$ محاسبه می‌کند، و برای دستیابی به یک گره قابل اعتماد، گره i با احتمال $c_{i,j}$ گره j را برای تراکنش برمی‌گزینند.

در Peer Trust [۶]، قابلیت اعتماد یک گره با ارزیابی آن گره در فراهم آوردن سرویس برای سایر گره‌ها در گذشته تعریف می‌شود. این مدل مقدار اعتمادی را که سایر گره‌های موجود در اجتماع در مورد گره داده شده براساس تجربه‌های گذشته خود دارند منعکس می‌کند. برای چنین ارزیابی پنج عامل تعریف می‌شود، که عبارتند از: فیدبکی که یک گره از سایر گره‌ها به دست می‌آورد، حوزه فیدبک مانند تعداد کل تراکنش‌هایی که یک گره با گره‌های دیگر دارد، قابل اطمینان بودن منبع فیدبک، محتوای تراکنش برای تفکیک تراکنش‌های بحرانی و غیر بحرانی و نهایتاً محتوای اجتماع[۷] برای نشان دادن خصوصیات و آسیب‌پذیری‌های وابسته به اجتماع. سپس با ترکیب عوامل مذکور، یک رابطه عمومی اعتماد به دست می‌آورد. RFSN، ATRM و CORE نیز از جمله مدل‌های اعتمادی هستند که بر روی شبکه‌های حسگر بیسیم گسترش یافته‌اند [۹، ۱۱].

در مدل اعتماد پیشنهادی (DSTM) هر گره مقدار اعتماد گره‌هایی را که در محدوده رادیویی آن قرار دارند، براساس تراکنش‌های قبلی و از دو طریق مستقیم و غیرمستقیم به دست می‌آورد و از ساختار کلی شبکه اطلاع ندارد. از سوی دیگر این مدل نیاز به یک سرور مرکزی برای نگه‌داری مقادیر اعتماد نداشته که این امر به خوبی با شبکه‌های حسگر بیسیم سازگار است.

۳- فرضیات و توصیف کلی مدل DSTM

انواع مختلفی از شبکه‌های حسگر بیسیم با توجه به نوع گره‌های تشکیل دهنده آن‌ها وجود دارد. در یک دسته‌بندی شبکه‌ها به دو دسته ایستا و پویا تقسیم می‌شوند، در شبکه‌های ایستا گره‌ها مکان مشخصی دارند و در شبکه‌های پویا گره‌ها به هر جایی حرکت می‌کنند. در دسته‌بندی دیگر می‌توان شبکه‌های حسگری را داشت که گره‌ها برای صرفه‌جویی در مصرف انرژی در مواقع بیکاری، به حالت غیرفعال[۸] می‌باشند. در این مقاله بدون از بین رفتن کلیت مسأله فرض می‌شود برخی از گره‌ها تقاضاکننده سرویس (یا کلاینت) هستند و برخی دیگر فراهم‌آورنده سرویس (یا سرور) 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 DSTM، هر گره از دو منبع برای به دست آوردن مقادیر اعتماد گره‌های همسایه‌اش استفاده می‌کند، اولاً مقدار اعتماد مستقیم گره مورد نظرش را می‌داند و ثانیاً در مورد آن گره اعتماد غیرمستقیمی را که توسط سایر گره‌های مشترک در محدوده رادیویی هر دو گره به دست می‌آید، 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 و خواص اعتماد در مورد آن برقرار است.

در DSTM در مرحله راه‌اندازی سامانه مدیریت، 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.

در این مدل اعتماد هر گره اعتماد مستقیم سایر گره‌هایی را که در محدوده رادیویی آن قرار دارند، نگه می‌دارد این موضوع با توجه به شکل ۱ مشخص می‌شود. در این شکل گره ۱ مقدار اعتماد گره‌های ۲، ۳، ۴، ۵، ۶ و ۷ را نگه می‌دارد. مقدار اعتماد مستقیم گره i به گره j در مرحله n با $T_{ij}(n)$ که $i,j=1,2,3,...$ نشان داده می‌شود.

برای محاسبه اعتماد غیرمستقیم، اگر گره i بخواهد اعتماد غیرمستقیم گره j را به دست آورد، باید از مقدار اعتمادی که سایر گره‌ها در مورد گره j دارند استفاده کند ولی از آن‌جا که هر گره فقط اعتماد گره‌های همسایه‌اش را نگه‌داری می‌کند تنها گره‌هایی می‌توانند به گره i در به دست آوردن اعتماد غیرمستقیم کمک کنند، که در محدوده رادیویی مشترک گره‌های i و j قرار داشته باشند. برای مثال 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 از این دو گره استفاده می‌کند.

اعتماد غیرمستقیم گره i به گره j در مرحله n با $R_{ij}(n)$ نشان داده می‌شود. اگر گره i بخواهد مقدار اعتماد غیرمستقیم گره j را به دست آورد، مقدار اعتماد مستقیم سایر گره‌ها در مورد گره j را سؤال می‌کند و با توجه به اعتمادی که خودش در مورد گره‌های پاسخ‌دهنده دارد اعتماد غیر مستقیم گره مذکور را با رابطه (۱) محاسبه می‌کند.

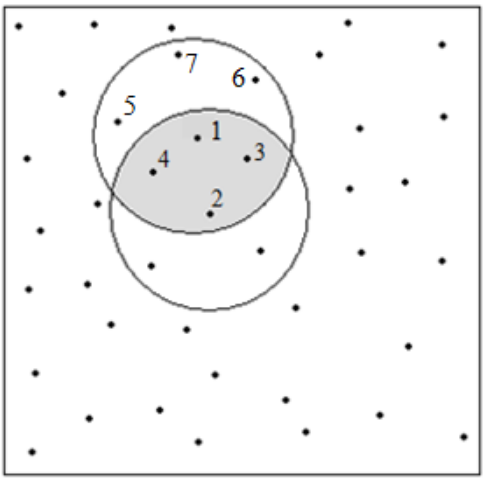
$$R_{ij}(n)=\frac{1}{N_{ij}}\sum_{k}T_{ik}*T_{kj} \qquad (۱)$$

در رابطه ۱، N_{ij} تعداد گره‌های موجود در محدوده مشترک بین گره i و j است و k شماره آن گره‌ها است. در مثال شکل ۱، اگر $i=1$ و $j=2$ در نظر گرفته شوند، $N=2$ و $k=3,4$ است.

در نهایت برای محاسبه اعتماد کلی هر گره باید اعتماد مستقیم و غیرمستقیمی را که در مراحل قبل به دست آورده با هم ترکیب کند و یک مقدار اعتماد کلی برای هر یک از همسایگانش در نظر بگیرد. اعتماد کلی گره i به گره j با $T'_{ij}(n)$ نشان داده می‌شود و از رابطه ۲ به دست می‌آید.

$$T'_{ij}(n) = w_1 T_{ij}(n) + w_2 R_{ij}(n) \quad (۲)$$

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، و با توجه به شرایط محیطی و چگونگی عملکرد گره‌ها تغییر می‌کنند.



شکل ۱- گره ۱ اعتماد مستقیم گره‌های ۲، ۳، ۴، ۵، ۶، ۷ را نگه می‌دارد و برای به دست آوردن اعتماد غیرمستقیم گره ۲ از گره‌های ۳ و ۴ که در محدوده رادیویی مشترک گره‌های ۱ و ۲ قرار دارند، کمک می‌گیرد.

۳-۱- به روز کردن مقدار اعتماد

چگونگی به روز شدن مقدار اعتماد در شبکه، 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، این گره مقدار اعتماد تمام گره‌های همسایه‌اش را با روشی که در بالا ذکر شد محاسبه می‌کند و برای دریافت سرویس از طریق گره‌ای که بالاترین مقدار اعتماد را دارد اقدام می‌کند. پس از دریافت سرویس، گره i سرویس دریافتی را با سرویس مورد تقاضا مقایسه می‌کند و با توجه به رضایت خود از سرویس دریافتی، مقدار اعتماد مستقیمی را که از گره همسایه دارد به روز می‌کند. رضایت گره i در مورد سرویس دریافتی در مرحله n با $S_i(n)$ نشان داده می‌شود. اگر i از سرویس دریافتی راضی باشد مقدار آن برابر ۱ و در غیر این صورت برابر صفر است.

۳-۲- پاداش و جریمه

همان‌طور که در بخش قبل بیان شد 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 و افزایش اعتماد با رابطه ۳ انجام می‌پذیرد.

$$T_{ij}(n+1) = \begin{cases} (1+\beta) * T_{ij}(n) & S_i(n+1) = 1 \\ (1-p\beta) * T_{ij}(n) & S_i(n+1) = 0 \end{cases} \quad (۳)$$

که در رابطه ۳، β عددی در بازه [۰، ۱] است و مقدار آن تأثیر چشمگیری در چگونگی عملکرد مدل اعتماد دارد. p ضریبی برای کنترل نرخ کاهش اعتماد می‌باشد. $S_i(n+1)$ رضایت گره i از سرویس دریافتی است. i گره تقاضاکننده سرویس و j گره‌ای است که دریافت سرویس از طریق آن صورت گرفته است.

۳-۳- به روز کردن اعتماد گره‌های دخیل در اعتماد غیرمستقیم

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 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.

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

در رابطه ۴، ε بسیار کوچکتر از β است، زیرا از آن‌جا که نمی‌توان از روی کیفیت سرویس دریافتی قضاوت کاملی در مورد تمام این گره‌ها داشت، 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.

۴- ارزیابی و تحلیل DSTM

همان‌طور که اشاره شد DSTM یک مدل اعتماد توزیع‌شده است که برخلاف سایر مدل‌های اعتماد توزیع‌شده که هر گره اعتماد کلیه گره‌هایی که قبلاً با آن‌ها تراکنش داشته است را نگه می‌دارد، در DSTM هر گره تنها اعتماد گره‌های همسایه خود را نگه می‌دارد. بنابراین می‌توان میزان توزیع‌شدگی آن را تعیین کرد و از سوی دیگر چون گره‌ها از چیدمان کلی شبکه اطلاعی ندارند این مدل قابل گسترش روی شبکه‌های با تعداد متفاوت گره حسگر است. در ادامه به بررسی بیشتر این موضوعات پرداخته می‌شود.

۴-۱- توزیع‌شدگی DSTM

ساختار کلی برای مدل‌های اعتماد و اعتبار شامل ساختارهای متمرکز و ساختارهای توزیع شده است [۱۲]. در ساختارهای متمرکز، یک مرکز اعتماد کلیه ارزیابی‌ها را جمع‌آوری می‌کند و یک نمره اعتماد را برای هر یک از اعضا محاسبه می‌نماید. تمام نمرات اعتماد به صورت عمومی در دسترس هستند و اعضا می‌توانند

هنگام تصمیم‌گیری در مورد تراکنش‌ها از این نمرات اعتماد استفاده کنند. در سیستم‌های توزیع‌شده، هر گره مقدار اعتماد تمام عناصری که قبلاً با آن‌ها تراکنش داشته است را نگه می‌دارد و زمانی که می‌خواهد تراکنش جدیدی را آغاز کند با توجه به آن‌چه خود در مورد سایرین می‌داند و اطلاعاتی که با سؤال کردن از بقیه به دست می‌آورد، تصمیم‌گیری می‌کند.

در DSTM هر گره مقدار اعتماد گره‌های همسایه خود را نگه می‌دارد، بنابراین DSTM یک مدل اعتماد توزیع‌شده است که میزان توزیع‌شدگی آن با توجه به شعاع رادیویی یک گره قابل کنترل است. زیرا تعداد گره‌های موجود در محدوده رادیویی یک گره و تعداد گره‌های موجود در محدوده رادیویی مشترک دو گره به r (شعاع رادیویی گره‌های حسگر) وابسته‌اند، از این‌رو می‌توان با توجه به شرایط موجود (مانند چگالی گره‌های حسگر) و نیازمندی‌های شبکه (مانند صرفه‌جویی در حافظه موردنیاز گره‌ها و ترافیک شبکه) میزان توزیع‌شدگی DSTM را تغییر داد.

اگر فرض شود چگالی گره‌های تشکیل‌دهنده یک شبکه حسگر برابر D است از آن جا که شعاع رادیویی هر گره حسگر r متر می‌باشد، هر گره می‌تواند محدوده‌ای به مساحت $\pi * r^2$ را پوشش دهد. تعداد گره‌هایی که در این محدوده قرار می‌گیرند از رابطه ۵ به دست می‌آید.

$$K = \pi r^2 * D \qquad (۵)$$

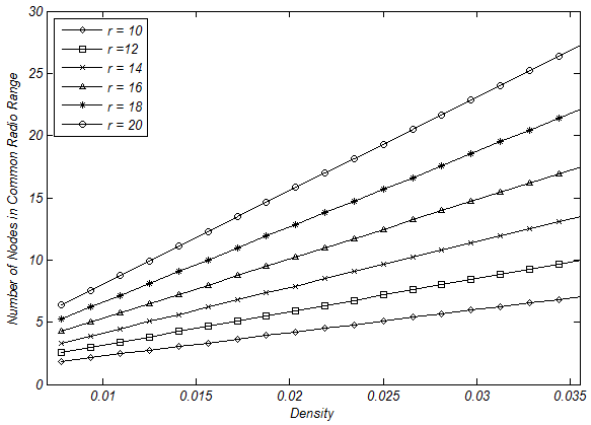
همان‌طور که در رابطه ۵ مشاهده می‌شود می‌توان با توجه به شرایط موجود در شبکه و چگالی گره‌ها با تغییر r، تعداد گره‌های موجود در محدوده رادیویی هر گره و به این ترتیب حافظه موردنیاز هر گره را کنترل کرد. برای مثال اگر چگالی زیاد باشد با کاهش شعاع رادیویی گره‌های حسگر می‌توان تعداد گره‌های موجود در محدوده رادیویی یک گره را کاهش داد.

قبلاً اشاره شد که گره i برای به دست آوردن مقدار اعتماد غیرمستقیم گره j، از اطلاعات گره‌های موجود در محدوده رادیویی مشترک گره‌های i و j استفاده می‌کند و به این ترتیب بخشی از ترافیک شبکه ناشی از رد و بدل شدن اطلاعات مربوط به محاسبه اعتماد غیرمستقیم گره‌ها است. تعداد گره‌های موجود در محدوده رادیویی مشترک گره‌های i و j با استفاده از رابطه ۶ به دست می‌آید.

$$N_{ij} = D\left[(2r^2 \cos^{-1}(\frac{d_{ij}}{2r})) - (\frac{d_{ij}}{2})\sqrt{4r^2 - {d_{ij}}^2})\right] \qquad (۶)$$

برای به دست آوردن مقدار $N_{i,j}$ در شبکه‌های با تعداد مختلف گره حسگر و حسگرها با شعاع رادیویی متفاوت از نرم‌افزار MATLAB استفاده شد. شرایطی که برای شبیه‌سازی فرض شده است به این ترتیب می‌باشد: محدوده‌ای که گره‌های حسگر در آن پخش شده‌اند دارای ابعاد $80m \times 80m$ است و گره‌ها به صورت ایستا هستند. سپس با فرض توزیع یکنواخت گره‌ها در شبکه، میانگین فاصله هر گره از همسایه‌هایش محاسبه می‌گردد و پس از متوسط‌گیری روی کل گره‌های موجود در شبکه با استفاده از رابطه ۶ تعداد گره‌های موجود در محدوده رادیویی مشترک دو گره به دست می‌آید. با تکرار آزمایش‌ها برای شعاع‌های رادیویی مختلف شکل ۲ به دست آمد. شایان ذکر است هر یک از منحنی‌ها نتیجه متوسط‌گیری روی ۵۰ بار تکرار آزمون است.

با توجه به این‌که تعداد گره‌های موجود در محدوده رادیویی مشترک دو گره نشان‌دهنده حجم اطلاعات مبادله‌شده برای محاسبه اعتماد غیرمستقیم می‌باشد، اگر خواسته شود که حجم اطلاعات مبادله‌شده برای محاسبه اعتماد غیرمستقیم از میزان مشخصی کمتر باشد که این امر در به‌کارگیری مدل ارائه شده در شبکه‌های حسگر مهم می‌باشد، باید تعداد گره‌های موجود در محدوده رادیویی مشترک دو گره کاهش یابد. در این شرایط چنانچه شعاع رادیویی گره‌های حسگر ثابت باشد، در شکل ۲ براساس حداکثر حجم مبادله ممکن می‌توان حداکثر چگالی را یافت، و به طور معکوس اگر چگالی مشخصی از گره‌های حسگر مد نظر باشد می‌توان شعاع رادیویی حسگرها را تعیین نمود. شایان ذکر است امکان کنترل ترافیک ناشی از



شکل ۲- تعداد گره‌های موجود در محدوده رادیویی مشترک دو گره بر حسب چگالی گره‌های حسگر به ازای شعاع‌های رادیویی مختلف.

مبادله اطلاعات مربوط به محاسبه اعتماد از ویژگی‌های این مدل است که ناشی از توزیع‌شدگی عملیات محاسبه اعتماد می‌باشد و در سایر مدل‌ها به این صورت وجود ندارد.

۴-۲- مقیاس‌پذیری DSTM

از آن‌جا که در DSTM هر گره، تنها اعتماد گره‌های همسایه خود را نگه می‌دارد و اطلاعی در مورد ساختار کلی شبکه ندارد، می‌توان آن را در شبکه‌هایی که دارای تعداد مختلف گره حسگر هستند به کار برد.

برای ارزیابی مقیاس‌پذیری DSTM از شبیه‌سازی با نرم‌افزار TRMSim-WSN استفاده شده است [۱۳]. TRMSim-WN یک شبیه‌ساز مأخذ آزاد[۹] مدل‌های اعتماد و اعتبار برای شبکه‌های حسگر بیسیم است. این شبیه‌ساز براساس زبان برنامه‌نویسی جاوا توسعه یافته است و می‌توان مدل‌های اعتماد جدید را به آن اضافه نمود.

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 گردید. در هر شبکه تعداد گره‌های کلاینت ثابت بوده و برابر ۷۵٪ کل گره‌ها است و ۲۵٪ بقیه به صورت سرور عمل می‌کنند. درصد سرورهای بدخواه با M نشان داده می‌شود. همچنین شعاع رادیویی هر حسگر برابر ۱۵ متر و ابعاد منطقه مانند حالت قبل، برابر $80m \times 80m$ است. با تغییر M از ۱۰٪ تا ۹۰٪ در هر شبکه، میزان دستیابی کلاینت‌ها به سرورهای قابل اعتماد به دست آمد، به این صورت که هر کلاینت ۵۰ مرتبه تقاضای سرویس می‌کند و میانگین دستیابی کلاینت‌ها به سرورهای قابل اعتماد در ۱۰۰ شبکه مورد آزمون اندازه‌گیری گردید. با تکرار شبیه‌سازی‌ها برای $N = 50,100,150,200$ نتایج نشان داده شده در شکل ۳ به دست آمد.

با توجه به شکل ۳ اولین نکته قابل توجه شباهت بین درصد انتخاب سرورهای قابل اعتماد، صرف‌نظر از تعداد گره‌های تشکیل‌دهنده شبکه است، که بیان‌کننده مقیاس‌پذیری مدل اعتماد پیشنهادی است. به این مفهوم که مدل اعتماد

پیشنهادی در شبکه‌های با تعداد مختلف گره حسگر به صورت یکسانی عمل می‌کند به خصوص اگر M (درصد سرورهای بدخواه) در شبکه کمتر از ۴۰٪ باشد کلیه نمودارها مقادیر تقریبا یکسانی دارند و مدل اعتماد پیشنهادی تمام آن‌ها به یک شکل عمل می‌کند. موضوع دیگری که می‌توان از شکل ۳ استنباط کرد این است که زمانی‌که درصد گره‌های بدخواه از ۵۰٪ کمتر باشد، درصد انتخاب سرورهای قابل اعتماد بالاتر از ۹۰٪ است. شایان ذکر است با تکرار شبیه‌سازی‌ها و تغییر شرایطی مانند شعاع رادیویی گره‌های حسگر و ابعاد منطقه نتایج مشابهی حاصل شد.

به منظور این‌که مدل اعتماد قابل قبول باشد، باید درصد انتخاب سرورهای قابل اعتماد از اندازه مشخصی، برای مثال ۸۰٪ بیشتر باشد و اگر درصد انتخاب سرورهای قابل اعتماد از این مقدار کمتر باشد نشان‌دهنده ناکارایی مدل است.

با توجه به شکل ۳ 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 درصدسرورهای بدخواه کمتر از ۷۰٪ باشد، درصد انتخاب سرورهای 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 بیسیم با تعداد کمتر گره، این مدل در حضور درصد بالایی از سرورهای بدخواه همچنان به خوبی عمل می‌کند.

شکل ۳ میانگین درصد انتخاب سرورهای قابل اعتماد را نشان می‌دهد. اما برای مثال میانگین ۸۰٪ می‌تواند به این دلیل به دست آید که این مدل اعتماد در کلیه شبکه‌ها با N گره، در ۸۰٪ موارد به سرور قابل اعتماد دست می‌یابد و یا این‌که مدل در نیمی از شبکه‌های مورد آزمایش در ۱۰۰٪ موارد به سرور قابل اعتماد دست می‌یابد و در نیم دیگر شبکه‌ها در ۶۰٪ موارد سرور قابل اعتماد را به دست می‌آورد.

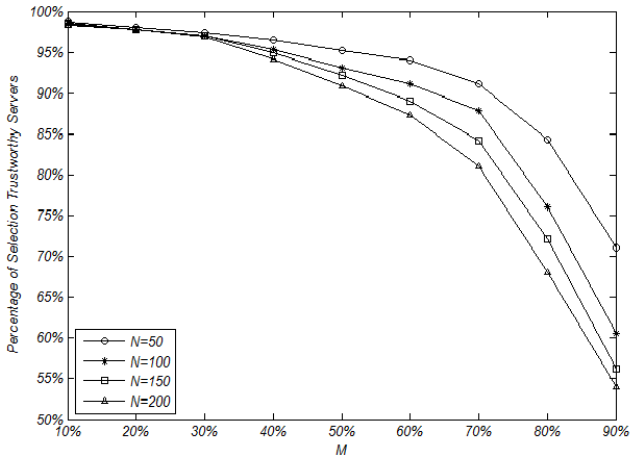
در شکل ۴ نیز شباهت کلیه نمودارها که برای شبکه‌ها با چگالی‌های مختلف به دست آمده‌اند، مشاهده می‌شود. به خصوص در حالتی که درصد گره‌های بدخواه کمتر از ۵۰٪ باشد، انحراف معیار عدد کوچکی بوده و برای تمامی نمودارها مقدار تقریباً یکسانی دارد. این موضوع بدان معنی است که زمانی‌که درصد سرورهای بدخواه در شبکه کمتر از ۵۰٪ باشد، مدل اعتماد پیشنهادی می‌تواند با توجه به شکل ۳ در شبکه‌های با تعداد مختلف گره به سرورهای قابل اعتماد دست یابد، بدون این‌که به ساختار آن‌ها وابسته باشد.

با توجه به شکل ۴، 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 چگالی کمتر DSTM به ساختار شبکه تحت آزمایش وابسته است.

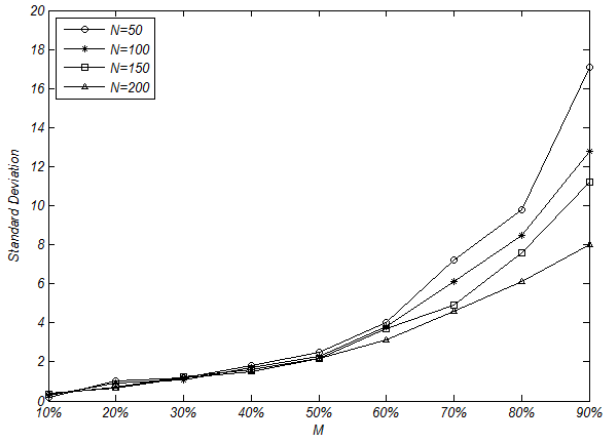
به طور خلاصه می‌توان بیان کرد اگر چگالی گره‌های شبکه حسگر کم باشد، وابستگی این مدل اعتماد به ساختار شبکه و چگونگی قرار گرفتن گره‌ها نسبت به یکدیگر بیشتر از حالتی است که چگالی شبکه زیاد است. بنابراین برای شبکه‌های با چگالی بیشتر، DSTM وابستگی کمتری به ساختار شبکه دارد.

۵- نتیجه‌گیری و کارهای آینده

پژوهش‌های موجود در مورد امنیت شبکه‌های حسگر بیسیم اغلب با فرض یک محیط مورد اعتماد ایجاد می‌شوند، از این‌رو مفهوم مدیریت اعتماد که اعتماد را در رفتار عناصر شبکه مدل می‌کند می‌تواند به خصوص برای شبکه‌های حسگر بیسیم مفید باشد.



شکل ۳- میزان دستیابی کلاینت‌ها به سرورهای قابل اعتماد در شبکه‌های حسگر با تعداد گره‌های متفاوت، به ازای تغییر درصد سرورهای بدخواه



شکل ۴- انحراف معیار درصد انتخاب سرورهای قابل اعتماد برای شبکه‌های حسگر با تعداد مختلف گره

مدل‌های اعتماد می‌توانند برای آشکارسازی گره‌ای که به درستی رفتار نمی‌کند استفاده شوند. در این مقاله یک مدل اعتماد توزیع‌شده و مقیاس‌پذیر برای شبکه‌های حسگری که به صورت کلاینت و سرور 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 تطبیقی در هر مرحله به روز و به مقدار واقعی نزدیک می‌کند. مشاهده شد که میزان توزیع‌شدگی این مدل اعتماد با توجه به شرایط می‌تواند توسط شعاع رادیویی گره‌ها کنترل شود و بنابراین مقدار حافظه موردنیاز هر گره قابل کنترل است. از سوی دیگر با توجه به این‌که بخشی از ترافیک شبکه ناشی از رد و بدل شدن اطلاعات برای محاسبه اعتماد غیرمستقیم گره‌ها است، می‌توان با توجه به شرایط با تغییر شعاع رادیویی گره‌ها این ترافیک را کنترل نمود. همچنین شبیه‌سازی‌ها نشان می‌دهد که اگر تعداد سرورهای بدخواه در شبکه، کمتر از ۵۰٪ کل سرورها باشد صرف نظر از تعداد گره‌های شبکه، میزان دستیابی کلاینت‌ها به سرورهای قابل اعتماد بالاتر از ۹۰٪ است.

برای بررسی بهتر چگونگی عملکرد DSTM در آینده می‌توان مقاومت آن را در برابر حملات رایج در شبکه بررسی کرد. همچنین در DSTM هر گره تنها از اطلاعات خود و اطلاعات همسایه‌های مستقیم خود استفاده می‌کند، می‌توان این مدل را به این صورت گسترش داد که هر گره علاوه بر این دو منبع، از گره‌هایی که در همسایگی هر یک از همسایه‌هایش قرار دارند نیز کمک بگیرد.

مراجع

[1] F. G´omez M´armol, and G. Mart´ınez P´erez, "Providing Trust in Wireless Sensor Networks using a Bio-inspired Technique," *Proc. of the Networking and Electronic Commerce Research Conference*, pp. 312-321, 2008.

[2] J. Hur, Y. Lee, S. Hong, and H. Yoon, "Trust-Based Secure Aggregation in Wireless Sensor Networks," *Proc. of the 3rd International Conference on Computing, Communications and Control Technologies*, pp. 159-165, 2005.

[3] L. Hu, and D. Evans, "Secure Aggregation for Wireless Networks," *Proc. of the Workshop on Security and Assurance in Ad hoc Networks*, pp. 384-391, 2003.

[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," *Proc. of the IEEE Symposium on Security and Privacy*, pp. 259-272, 2004.

[5] G. Han, L. Shu, J. Hyuk Park, and J. Ni, "Power-Aware and Reliable Sensor Selection Based on Trust for Wireless Sensor Networks," *Journal of Communications*, vol. 5, no. 1, pp. 23-30, 2010.

[6] L. Xiong, and L. Liu, "PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities," *IEEE Transactions on Knowledge and Data Engineering*, pp. vol. 16, no. 7, pp. 843–857, 2004.

[7] R. Zhoh, and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer to Peer Computing," *IEEE Transaction on Parallel and Distributed Systems*, vol. 18, no. 4, pp. 460-473, 2007.

[8] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," *Proc. of the International World Wide Web Conference*, pp. 173-186, 2003.

[9] S. Ganeriwal, and M. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," *Proc. of the ACM workshopon Security of Ad-hoc and Sensor networks*, pp. 66-77, 2004.

[10] S. Buchegger, and J. Y. Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," *Proc. of the Workshop on the Economics of Peer-to-Peer Systems*, pp. 83-89, 2004.

[11] Y. Sun, and Y. Yang, "Trust Establishment in Distributed Networks: Analysis and Modeling," *Proc. of the IEEE International Conference on Communications and Information Systems Security Symposium*, pp. 1266-1273, 2007.

[12] A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation for Online Service Provision," *Proc. of Emerging issues in Collaborative Commerce*, pp. 618-644, 2007.

[13] F. Gómez, and G. Martínez, "TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks," *Proc. of the Communication and Information Systems Security Symposium*, pp. 545-552, 2009.

خدیجه نخعی مدرک کارشناسی‌ارشد خود را در رشته مهندسی فناوری اطلاعات- مخابرات امن از دانشگاه علم و صنعت ایران و مدرک کارشناسی خود را در رشته مهندسی برق- مخابرات از دانشگاه صنعتی اصفهان دریافت نموده است. موضوعات مورد علاقه وی شبکه‌های بیسیم، امنیت شبکه‌ها و روش‌های برقراری امنیت می‌باشد.

آدرس پست‌الکترونیکی ایشان عبارت است از:

kh_nakhaei@ee.iust.ac.ir

هادی شهریار شاه‌حسینی عضو هیأت علمی دانشکده مهندسی برق دانشگاه علم و صنعت ایران می‌باشد. زمینه‌های فعالیت‌های تخصصی ایشان طراحی پردازنده‌های سریع، ابررایانش و شبکه است. از نتایج تحقیقات وی تا کنون بیش از ۱۳۰ مقاله علمی در مجلات و مجموعه مقالات کنفرانس‌های معتبر علمی به چاپ رسیده است. ایشان از سال ۱۳۷۸ عضو کمیته اجرائی و هماهنگ کننده فعالیت‌های منطقه‌ای در حوزه کشورهای خاورمیانه در IEEE TFCC و پس از آن IEEE TCSC است و در نوامبر ۲۰۰۷ میلادی لوح تقدیر انجمن کامپیوتر IEEE بدلیل فعالیت‌های مستمر و مؤثر او بعنوان هماهنگ کننده منطقه‌ای IEEE در حوزه خاورمیانه به وی اعطا گردید.

آدرس پست‌الکترونیکی ایشان عبارت است از:

hshsh@iust.ac.ir

اطلاعات بررسی مقاله:

تاریخ ارسال: ۸۹/۳/۲۴

تاریخ اصلاح: -

تاریخ قبول شدن: ۸۹/۱۰/۷

نویسنده مرتبط: دکتر هادی شهریار شاه‌حسینی، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران، ایران.

[1] Eavesdropping
[2] Denial of Service
[3] Collusion
[4] Oscillating Behavior
[5] MAC: Message Authentication Code
[6] Distributed & Scalable Trust Model
[7] Community Context
[8] Idle
[9] Open Source